

UNIVERSITÉ DU QUÉBEC À MONTRÉAL

L'ÉVOLUTION DU DROIT À L'OUBLI NUMÉRIQUE

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN DROIT INTERNATIONAL

PAR
LOUIS D. PASQUIN

Août 2022

UNIVERSITÉ DU QUÉBEC À MONTRÉAL
Service des bibliothèques

Avertissement

La diffusion de ce mémoire se fait dans le respect des droits de son auteur, qui a signé le formulaire *Autorisation de reproduire et de diffuser un travail de recherche de cycles supérieurs* (SDU-522 – Rév.04-2020). Cette autorisation stipule que «conformément à l'article 11 du Règlement no 8 des études de cycles supérieurs, [l'auteur] concède à l'Université du Québec à Montréal une licence non exclusive d'utilisation et de publication de la totalité ou d'une partie importante de [son] travail de recherche pour des fins pédagogiques et non commerciales. Plus précisément, [l'auteur] autorise l'Université du Québec à Montréal à reproduire, diffuser, prêter, distribuer ou vendre des copies de [son] travail de recherche à des fins non commerciales sur quelque support que ce soit, y compris l'Internet. Cette licence et cette autorisation n'entraînent pas une renonciation de [la] part [de l'auteur] à [ses] droits moraux ni à [ses] droits de propriété intellectuelle. Sauf entente contraire, [l'auteur] conserve la liberté de diffuser et de commercialiser ou non ce travail dont [il] possède un exemplaire.»

REMERCIEMENTS

Je tiens à exprimer ma gratitude à mon directeur de recherche, Me Philippe Fortin, professeur à l'UQAM, pour ses conseils très précieux et encouragements tout au long de ce travail. J'ai également apprécié sa généreuse disponibilité, ce qui a contribué à l'avancement de ce mémoire.

Je souhaite adresser mes affectueux remerciements à ma conjointe pour son soutien et son encouragement inconditionnels tout au long de mes études à la maîtrise. Merci également à Alexandra pour son inspiration et sa rigueur intellectuelle.

Enfin, je remercie l'Université du Québec à Montréal de m'avoir permis de réaliser mes études de maîtrise dans un environnement digne des plus hautes institutions d'enseignement.

AVANT-PROPOS

« L'Évolution du droit à l'oubli numérique » n'était pas le titre pour ce mémoire que nous avons d'abord choisi. À priori, la terminologie du « droit à l'oubli » manquait de précisions, particulièrement dans le cadre de notre étude du sujet qui adresse les questions de l'évolution de ce droit dans le contexte numérique. Pour nous, le droit aux « déréférencement » ou « à la désindexation » a l'avantage d'être plus clair et contemporain dans son application juridique pour désigner les différentes facettes de la mise en œuvre de « l'oubli », de certaines informations de personne sur Internet. Force est de constater que la littérature juridique ne semble pas s'en préoccuper autrement, probablement dû au fait que l'expression elle-même a une résonance acquise dans le langage juridique.

En général, les juristes emploient certains mots et expressions juridiques couramment utilisés dans leurs pratiques respectives, en supposant que leurs significations sont connues et bien établies, abstraction faite des cas particuliers, un peu comme un symbole linguistique invoquant une situation juridique précise.

Il est incontestable que le « droit à l'oubli » ou en anglais « the right to be forgotten » relève de la communication juridique commune pour désigner le déréférencement sur Internet.

C'est pour ces raisons que nous avons pris cette décision d'intituler le mémoire « L'évolution du droit à l'oubli numérique ». Il est donc important pour nous que le lecteur puisse identifier le sujet de la recherche par la simple lecture de son titre et d'éviter ainsi que l'ouvrage soit délesté par trop de technicité.

Soit dit en passant, le droit à l'oubli numérique est défini dans le prestigieux dictionnaire juridique français de Girard Cornu et est ainsi rédigé : « Oubli numérique (droit à l'). Droit d'exiger l'effacement sur Internet de données collectées, indexées, stockées et mises à la disposition de tiers, lorsque leur utilisation porte atteinte à la protection des données à caractère personnel et au respect de la vie privée ».

(Gérard Cornu, Vocabulaire juridique, 12^e éd., Paris, Presse universitaires de France, 2018).

Nous considérons, d'après notre étude évolutive du sujet, que le « droit à l'oubli numérique » du fait de son appellation est venu à représenter symboliquement la synthèse des droits relatifs à la protection des personnes à l'égard du traitement des données numériques à caractère personnel.

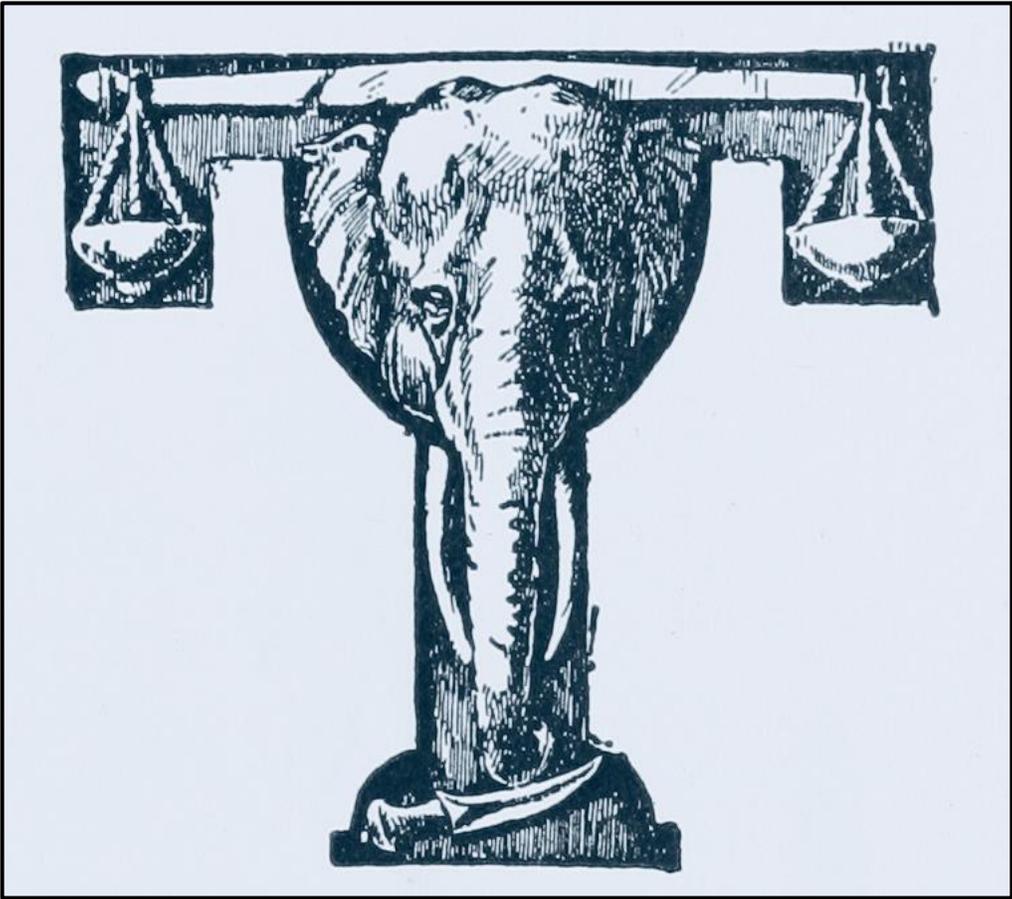


Image du domaine public, libre de droits et tirée du *Livre de la jungle* de W.H. Drake (publié en 1895)

TABLE DES MATIÈRES

REMERCIEMENTS	ii
AVANT-PROPOS	iii
RÉSUMÉ	ix
INTRODUCTION	1
CHAPITRE I.....	4
INFLUENCE EUROPÉENNE SUR L'ÉVOLUTION DU DROIT À L'OUBLI.....	4
1.1 Définition	4
1.2 Les deux formes du droit à l'oubli numérique	7
1.3 Genèse du droit à l'oubli numérique.....	12
1.4 Résolution 73(22) de 1973.....	16
1.5 La Directive 95/46/CE	18
1.6 Charte française sur le droit à l'oubli 2010.....	21
1.7 Le Règlement européen 2016/679	23
1.8 Droit à l'effacement (droit à l'oubli)	26
1.9 Le droit à l'oubli numérique n'est pas absolu.....	29
1.10 Charte des droits fondamentaux de l'Union européenne	31
1.11 Les décisions marquantes du droit à l'oubli	33
1.12 L'affaire Landru 1965	33
1.13 L'arrêt M. c. Filipacci 1983	34
1.14 L'affaire Google Spain	35
1.15 Pour un souci de clarté.....	36
1.16 Reconnaissance du droit à l'oubli par la CJUE	50
1.17 La cause emblématique d'une chirurgienne néerlandaise.....	52
1.18 Deux arrêts importants du 24 septembre 2019 de la CJUE	55
1.19 Mise en œuvre du droit à l'oubli en Europe	56
1.20 L'Arrêt c-136/17 de 2019	57
1.21 La portée territoriale du droit à l'oubli	63

1.21.1 L’arrêt c-507/17 de 2019	63
1.22 Sanction pour le non-respect du droit à l’oubli en Europe	71
1.23 Condamnation de Google à 50 millions d’euros.....	72
1.24 Amende historique pour le non-respect du droit à l’oubli	74
1.25 La sanction	77
1.26 Le droit à l’oubli constitue une obligation claire	78
CHAPITRE II	81
L’EVOLUTION DU DROIT À L’OUBLI AUX ÉTATS-UNIS, CANADA ET AU QUEBEC	81
2.1 L’ÉVOLUTION AUX ÉTAS-UNIS	83
2.1.1 Privacy Act de 1974.....	83
2.1.2 Cox Broadcasting Corp. C. Cohn	86
2.1.3 Oklahoma Publishing Co. c. Distric Court for Oklahoma County	87
2.1.4 Smith c. Daily Mail Publishing Co.	88
2.1.5 L’affaire Florida Star c. B.J.F	90
2.1.6 Projet de Loi le Data Care Act.	93
2.2 L’ÉVOLUTION AU CANADA	96
2.2.1 Liberté d’expression et l’équilibre avec la protection de la vie privée	98
2.2.2 Considération des principes à valeur constitutionnelle canadienne.....	99
2.2.3 Irwin Toy Ltd c. Procureur général du Québec	99
2.2.4 L’action gouvernementale et la liberté d’expression	100
2.2.5 Liberté d’expression n’est pas absolue	101
2.2.6 Aubry c. Éditions Vice-Versa Inc.....	101
2.2.7 Hill c. Église de scientologie	102
2.2.8 Grant c. Torstar Corp.	103
2.2.9 Loi sur la protection des renseignements personnels et des documents électroniques	103
2.2.10 Renvoi à la Cour fédérale 2021 CF 723	104

2.2.11	Loi sur la protection de renseignements personnels et des documents électroniques	107
2.2.12	Le neuvième principe – Accès aux renseignements et le droit à l’oubli.....	108
2.2.13	Projet de loi fédérale pour protection des renseignements personnels.....	109
2.2.14	La portée de la loi canadienne.....	110
2.2.15	Google Inc. C. Equustek Solutions Inc.	111
2.2.16	Douez c. Facebook Inc.	115
2.3	SITUATION AU QUÉBEC	117
2.3.1	C.L. c. BCF Avocats d’affaires.....	117
2.3.2	Projet de Loi no 64.....	118
2.3.4	<i>In fine</i>	120
2.3.5	Notions juridiques sous-jacentes au droit à l’oubli numérique : Distinction entre la protection de la vie privée et le droit à l’oubli	121
2.3.6	Le droit à l’oubli numérique et la liberté d’expression.....	123
	CONCLUSION	126
	BIBLIOGRAPHIE.....	129

RÉSUMÉ

L'être humain a la capacité de se souvenir et d'oublier, il est dit qu'il est difficile de se souvenir et facile d'oublier. Par carence, nous oublierions. La technologie numérique a permuté cela. Aujourd'hui, avec le stockage informatique abordable, quasi infini, une captation automatisée sans effort et un accès mondial, le souvenir est devenu la norme, pour nous et pour la société contemporaine.

Dans cet ouvrage, nous vous proposons une étude évolutive du droit à l'oubli dans le contexte numérique actuel, son application juridique mise en œuvre. La problématique retenue était donc de déterminer les assises historiques du droit à l'oubli, ces manifestations en droit positif contraignables et d'engager une réflexion prospective de ce droit. L'objet de cette étude n'est pas de savoir pourquoi des personnes veulent se faire oublier sur Internet, mais comment. Ainsi, nous avons orienté l'ensemble de la recherche sur l'oubli numérique en droit positif actuellement applicable, en droit européen, américain, canadien et québécois.

Dans le cadre de l'analyse de la problématique juridique du droit à l'oubli numérique, force est de constater qu'il peut difficilement être détaché de considérations qui débordent de l'unique question du traitement de données et d'Internet. Cela étant, nous avons également abordé les questions du droit au respect de la vie privée, la liberté d'expression et le droit à l'information.

Dans sa finalité, ce travail de recherche fait un suivi jurisprudentiel des décisions marquantes en rapport avec l'application concrète du droit à l'oubli numérique.

INTRODUCTION

À l’instar de l’adage voulant « qu’un éléphant n’oublie jamais, le réseau Internet, lui aussi, n’oublie jamais. »

En tant que personnes, nous avons la capacité de nous souvenir et d’oublier. Il est dit qu’il était difficile de se souvenir et d’oublier facilement. Par défaut, on finit par oublier. La technologie numérique a inversé cela. Car il est pratiquement impossible d’apprendre à un système informatique à oublier puisqu’il est conçu pour le stockage, le traitement et la récupération de données de manière automatisés, en conséquence l’oubli serait considéré comme un défaut technologique. Aujourd’hui, avec la collecte de données abordables, une récupération sans effort exécutée par des robots informatiques et un accès planétaire, le souvenir est devenu la norme par défaut, pour nous individuellement et sur l’ensemble de la société. Cette soif de données numériques alimentées par Internet qui génère un nombre de données incommensurables qui est essentiellement contrôlé par les GAFAM¹, les cinq grandes firmes américaines privées qui dominent le marché du numérique mondial.

Parallèlement à ce changement de société relié à l’innovation technologique et à l’économie numérique, les personnes commencent à se rendre compte de la somme de données livrées sur eux-mêmes et accessibles à tous. L’éveil vient du fait que leur présence

¹ Le terme GAFAM s’emploie dans le domaine de l’économie. C’est un acronyme formé avec les initiales des noms de cinq grandes entreprises américaines, souvent qualifiées de géants du Web : G pour Google, F pour Facebook, M pour Microsoft et les deux A pour Apple et Amazon.

Les GAFAM sont des entreprises d’envergure internationale, qui touchent des milliards d’utilisateurs et traitent une quantité phénoménale de données. Par ailleurs, elles jouent un rôle économique et financier considérable à l’échelle mondiale. Ces entreprises possèdent et contrôlent plusieurs réseaux sociaux et services Web très utilisés, comme LinkedIn (qui appartient à Microsoft), YouTube (à Google), Instagram et WhatsApp (à Facebook). Les cinq sociétés dites GAFAM ont une capitalisation boursière commune de plus de 4 billions de dollars en mai 2020. Il est intéressant de noter qu’elles sont également les cinq premières entreprises en termes de capitalisation boursière sur le NASDAQ. Parmi les actions des GAFAM, la plus ancienne société à être cotée en bourse est Apple, qui a fait son introduction en bourse en 1980, suivie de Microsoft en 1986, Amazon en 1997, Google en 2004 et Facebook en 2012. Voir le Dictionnaire Orthodidacte, Que veut dire le mot GAFAM, (20 juillet 2022), en ligne : <https://dictionnaire.orthodidacte.com/article/definition-gafam>

sur Internet laisse de traces. Il peut s'agir parfois d'information journalistique, notamment la participation d'évènement d'actualité.

Ou encore, référencer des informations par des entreprises exploitant des moteurs de recherche au profit de leur transmission vers les internautes. Les données personnelles peuvent également se retrouver facilement sur Internet par des informations partagées volontairement ou pas sur les réseaux sociaux par les intéressés qui diffusent eux-mêmes les informations personnelles la concernant. Il faut également mentionner que les géants du Web ont construit leurs modèles économiques basés sur la publicité ciblée à l'endroit des usagers d'Internet grâce aux données personnelles de ces derniers. Les données, même les plus insipides, sont pour eux une matière première après collecte. Les empreintes et les ombres d'une partie de nos vies qui se retrouvent sur le Web risquent à tout moment de refaire surface. Dans ce contexte, la protection des personnes physiques à l'égard du traitement des données personnelles est au centre de toutes les préoccupations. L'objet de cette étude n'est pas de savoir pourquoi des personnes veulent se faire oublier sur Internet, mais plutôt de s'interroger sur la manière dont l'oubli est présentement saisi par le droit. Ainsi, nous avons orienté l'ensemble de la recherche sur l'oubli numérique en droit positif actuellement applicable, en droit européen, américain et en droit canadien et québécois. Dans le cadre de l'analyse de la problématique juridique du droit à l'oubli numérique, force est de constater qu'il peut difficilement être détaché de considérations qui débordent de l'unique question du traitement de données et d'Internet. Cela étant, nous avons abordé les questions du droit au respect de la vie privée, la liberté d'expression et le droit à l'information.

Dès lors, les travaux menés ont rapidement permis de se convaincre que la question du droit à l'oubli dans le domaine numérique présente une évidente spécificité. Il suffit que votre nom soit mentionné sur des sites Internet, la liste de ces derniers s'affiche lorsque votre patronyme est saisi dans un moteur de recherche ou une plateforme numérique. Vous êtes ainsi référencé sans votre connaissance ni votre consentement. Le droit à l'oubli vous permet de vous y opposer, en conformité aux différentes législations étatiques d'ordre administratives développées ces dernières années. La problématique retenue était donc

celle de déterminer les assises historiques du droit à l'oubli, ces manifestations en droit positif contraignables et d'engager une réflexion sur le droit prospectif. Plutôt que s'attarder et de « fétichiser » sur le droit d'une personne identifiée ou qui peut être identifiée à gérer les renseignements personnels la concernant sur Internet ou d'autres valeurs tel que la liberté d'expression. Nous nous sommes plutôt attachés à déterminer l'évolution du droit à l'oubli numérique jusqu'à présent. Sur le plan philosophique, il nous semble que la citation de Friedrich Nietzsche est des plus appropriées pour présenter le sujet :

Toute action exige l'oubli, de même que toute vie organique exige non seulement la lumière, mais aussi l'obscurité. Un homme qui voudrait sentir les choses de façon absolument et exclusivement historique ressemblerait à quelqu'un qu'on aurait contraint à se priver de sommeil ou à un animal qui ne devrait vivre que de ruminer continuellement les mêmes aliments. Il est donc possible de vivre, et même de vivre heureux, presque sans aucune mémoire, comme le montre l'animal ; mais il est absolument impossible de vivre sans oubli. Ou bien, pour m'expliquer encore plus simplement sur mon sujet : il y a un degré d'insomnie, de rumination, de sens historique, au-delà duquel l'être vivant se trouve ébranlé et finalement détruit, qu'il s'agisse d'un individu, d'un peuple ou d'une civilisation².

² Friedrich Nietzsche, *Considérations inactuelles, II, "De l'inconvénient et de l'utilité pour la vie de l'histoire"*, 1874, tr. fr. Pierre Rusch, Folio essais, 1992, pp. 96-97

CHAPITRE I

INFLUENCE EUROPÉENNE SUR L'ÉVOLUTION À L'OUBLI NUMÉRIQUE

1.1 Définition

La Commission nationale de l'informatique et liberté de France le (CNIL) a défini le droit à l'oubli numérique comme « *La possibilité offerte à chacun de maîtriser ses traces numériques et sa vie en ligne, qu'elle soit privée ou publique* »³ et selon la revue analytique de la littérature juridique, le droit à l'oubli numérique est le droit à ce que les éléments relatifs au passé ou au présent d'une personne, d'une entreprise ou d'une marque de commerce (que ces éléments soient exacts ou inexacts, ou devenus obsolètes) puissent être retirés des contenus connectés à Internet ou qu'ils soient rendus difficilement accessibles, qu'ils soient extirpés de la mémoire numérique et qu'ils tombent dans l'oubli⁴. Mais encore, le droit à l'oubli numérique est le fruit de plusieurs années de travail des institutions européennes, à cette fin en 1995, l'Union européenne a adopté la directive sur la protection des données personnelles permettant de réglementer le traitement des données à caractère personnel et leur diffusion⁵. Le travail sur la directive a fait l'objet de modifications et d'adaptation en 2012, par la Commission européenne pour le droit à l'oubli⁶. C'est sur cette directive que la Cour de justice de l'Union européenne trouve ses assises dans une décision du 13 mai 2014 pour consacrer ce qui est désormais qualifié par l'appellation du « droit à

³ Commission Nationale de l'Informatique et Liberté de la France (CNIL), *Rapport d'activité 2013*, Documentation française, à la p 16.

⁴ Jean-Christophe Duton et Virginie Becht, « Le droit à l'oubli numérique : Un vide juridique ? », *Le journal du Net* (24 février 2010), en ligne : <<http://www.journaldunet.com/ebusiness/45246/le-droit-a-l-oubli-numerique-un-vide-juridique.shtml>>; Jeff Ausloos, « The « Right to be Forgotten » - Worth Remembering ? », (2012) 28 Computer L & Sec Rev 143 à la p 152 ; Marc Rees, « Droit au déréférencement : les critères de la CNIL pour se faire oublier sur Google » (28 novembre 2014), en ligne (blogue) : <<https://www.nextinpact.com/article/16169/91147-droit-au-dereferencement-criteres-cnil-pour-se-faire-oublier-sur-google>>

⁵ Directive 95/46/CE du Parlement européen et du conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J O n° L28, 23.11.1995 pp 31-50, en ligne : <<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046>>

⁶ Bruxelles, le 25 janvier 2012- La Commission européenne a proposé, ce jour, une réforme globale des règles adoptées par l'UE en 1995 en matière de protection des données afin de renforcer les droits en matière de respect de la vie privée dans l'environnement en ligne et de donner un coup d'accélérateur à l'économie numérique européenne. Les progrès technologiques et la mondialisation ont modifié en profondeur les modes de collecte, de consultation et d'utilisation de nos données.

l'oubli »⁷. La Cour de justice de l'Union européenne (CJUE) définit ce droit comme l'obligation pour un moteur de recherche de « supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages Web, publiée par des tiers et contenant des informations relatives à cette personne »⁸.

Dans les faits, le droit à l'oubli numérique, tel que défini par la Cour de justice de l'Union européenne en 2014 ne permet pas à une personne de demander aux opérateurs de moteur de recherche ou à l'hébergeur de supprimer des pages, mais permet de demander la suppression des liens. Les pages Web existent toujours, mais ne sont plus référencées. Lorsqu'on effectue une recherche à partir d'un nom de personnes, des liens vers les pages Web, publiés par des tiers et contenant les informations sur cette personne, existent déjà. En conséquence, ce sont les liens entre la recherche et la personne qui doivent être supprimés.

Autrement dit, le déréférencement est la solution proposée par la Cour de justice de l'Union européenne⁹. En effet, il suffit aux moteurs de recherche de ne plus renvoyer à la page Web où se trouvent les données que l'on veut oublier, même si les mots-clés nous y conduisent, ainsi les données sensibles ne sont plus accessibles. La contestation de cette définition du droit à l'oubli vient du fait que l'information n'est aucunement supprimée et reste accessible, par d'autres voies, que ce soit en utilisant d'autres mots-clés lors de la recherche, ou au moyen de différents sites ayant un lien vers la page relative à l'information sensible¹⁰.

⁷ Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD) et Mario Costeja González, CJUE, 13 mai 2014, C131/12, Arrêt de la Cour (grande chambre), en ligne : <<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62012CJ0131>> [Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD)].

⁸ *Ibid* au para 82.

⁹ *Ibid*.

¹⁰ Déférencement ne signifie pas l'effacement de l'information sur le site Internet source. Voir Stéphane Dreyfus, « La présidente de la Commission nationale de l'informatique et des libertés (CNIL) se réjouit de la décision européenne imposant un droit à l'oubli numérique, nouvelle arme à la disposition des citoyens », *La Croix* n° 39983, 12 septembre 2014, 11.

La nécessité d'une définition générale du droit à l'oubli numérique consacrée par la Cour de justice de l'Union européenne dans l'affaire Gonzales¹¹ est très importante pour reconnaître les assises juridiques de ce droit au-delà de la notion morale symbolique. L'actualisation d'un véritable droit comportant des conséquences civiles en cas de violation, une personne peut donc demander réparation¹². L'Internet a modifié notre mode de vie de façon considérable ces dernières années, il est tout à fait normal que le droit ait évolué pour intégrer cette technologie et l'encadrer juridiquement. C'est ainsi que des notions juridiques nouvelles sont apparues, à l'exemple du droit à l'oubli numérique. Comme l'exprime si bien Victor Mayer-Schoenberger dans un document de recherche publié par l'Université Harvard en 2007, qui peut être résumé de la façon suivante : « en tant qu'êtres humains, nous avons la capacité de nous souvenir et d'oublier ». Pendant des millénaires, ce souvenir était difficile et oublié beaucoup plus facilement. On oublierait par défaut. La technologie numérique et plus particulièrement l'Internet a renversé cela. Aujourd'hui, avec un stockage quasi illimité de données, une récupération sans effort et un accès mondial interconnecté, la mémoire est devenue par défaut, pour nous individuellement et la collectivité dans son ensemble¹³. L'expression « droit à l'oubli » semble être passée dans le langage commun, intégrée par différents acteurs du droit et de la politique à une prérogative légale qui mérite le qualificatif de « droit ».

Ce droit permet d'avoir un certain contrôle sur l'information qui circule en ligne sur une personne, une entreprise ou une marque de commerce¹⁴. En effet, il est actuellement des plus aisé d'entrer le nom d'une personne sur des moteurs de recherche comme Google, Bing ou Yahoo, etc. pour obtenir rapidement des informations sur celle-ci. Devenue courante, cette pratique est à même de porter atteinte au respect de la vie privée ou de diffuser des informations erronées, nuisibles ou obsolètes. Dans ce contexte, le droit à l'oubli numérique étant souhaitable, il en va de la nécessité de l'encadrer juridiquement

¹¹ [Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD)] *supra* note 7.

¹² *Ibid.*

¹³ Mayer-Schoenberger, Viktor and Mayer-Schoenberger, Viktor, "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing" (April 2007). KSG Working Paper No. RWP07-022, Available at SSRN: <<https://ssrn.com/abstract=976541>> or <<http://dx.doi.org/10.2139/ssrn.976541>>

¹⁴ Ausloos, *supra* note 4 à la p 152

afin de voir à son application au bénéfice de toutes personnes, qui ainsi cherchent à se faire oublier¹⁵.

1.2 Les deux formes du droit à l'oubli numérique

Il y a les deux formes du droit à l'oubli numérique : le droit au déréférencement et le droit à l'effacement. Le droit au déréférencement permet de demander à l'exploitant d'un moteur de recherche la suppression des résultats de recherche et des liens contenant des informations référencées¹⁶. La suppression de ces résultats par le moteur de recherche est donc envisageable, indépendamment d'un éventuel effacement des informations sur les sites Internet sur lesquels elles ont été publiées¹⁷.

Pris au pied de la lettre, le droit à l'effacement permet de demander à l'éditeur d'un site Internet d'effacer des données potentiellement nuisibles, lorsqu'il n'existe plus de raison légitime pour les diffuser ou les conserver. L'effacement équivaut à la suppression pure et simple des données pour oublier, il faut les effacer¹⁸. Une personne peut demander directement au site Internet, ou à celui qui détient les données, de retirer celle-ci. Le droit de demander que les données ou l'information soient ainsi effacées en temps et lieu est également une solution à l'oubli numérique¹⁹.

¹⁵ *Ibid* à la p 10.

¹⁶ Cécile De Terwangne, « Internet Privacy and the Right to Be Forgotten/Right to Oblivion » (2012) VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet" [monograph online]. *IDP. Revista de Internet, Derecho y Política*. No. 13, pp. 109-121. UOC.

¹⁷ *Ibid* à la p 169.

¹⁸ Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows. A Critical Analysis of the 'Right to be Forgotten' in big data practice", (2011) 8 :3 Scripted 229 à la p 240, en ligne : <https://script-ed.org/article/forgetting-footprints-shunning-shadows/>

¹⁹ De Terwangne, *supra* note 16; Edward L. Carter, "Argentina's Right to be Forgotten", (2013) 27 Emory Int'l L. Rev. 23, à la p 30 en ligne: <<https://scholarlycommons.law.emory.edu/eilr/vol27/iss1/3>>. Sur le même sujet, voir Norberto Nuno Gomes De Andrade, « Oblivion: The Right to be Different...from Oneself Reproposing the Right to be Forgotten » dans Alessia Ghezzi et al. *The Ethics of Memory in a Digital Age, Interrogating the Right to be Forgotten*, London, Palgrave Macmillan London, 2014, 65.

Comme on peut le constater, le droit à l'oubli numérique est une notion juridique faussement simple et la première difficulté est sans doute la définition même de ce droit. Comme déjà discuté en substance, il y a deux cas de figure, à savoir la possibilité de supprimer simplement les données sur un site Internet, ce que l'on nomme « droit à l'effacement » et celle de désindexer les données sur un moteur de recherche, ce qui est désigné comme « droit au déréférencement ». Bien que ces deux éléments concernent les données numériques sur une plateforme Internet, elles n'ont pas les mêmes provenances ni les mêmes résultats²⁰. En effet, il est tout à fait envisageable que les données soient supprimées d'un site Internet précis, tout en persistant de générer un résultat sur un moteur de recherche ou autre plateforme. Pareillement, le fait de déréférencer un lien vers une page ou un site Internet d'un moteur de recherche n'équivaut pas à la suppression de cette page ou de ce site²¹. Toujours est-il, les lois et la jurisprudence européenne en matière de protection des données personnelles garantissent aux personnes un droit à l'oubli sous ces deux notions juridiques. Cela émerge de l'arrêt Google Spain du 13 mai 2014 (l'affaire Gonzalez) de la Cour de justice de l'Union européenne²², pareillement, l'article 17 du règlement général sur la protection des données qui est directement lié à la problématique de l'oubli numérique et exécutoire²³.

De la première proposition du droit à l'oubli numérique, à savoir la suppression pure et simple des données est pour certains juristes la seule solution capable d'apporter le résultat juridique attendu, selon Gérard Hass²⁴. Pourtant, cette solution serait inappropriée pour plusieurs raisons. En premier lieu, l'affrontement entre les droits de liberté d'expression,

²⁰ De Terwangne, *supra*, note 19.

²¹ *Ibid.*

²² [Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD)], *supra* note 7.

²³ Article 17 du Règlement général sur la protection des données (RGPD) du 23 mai 2018; Voir Règlement (UE) 2016/679 du Parlement européen et du Conseil du 2 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données); lequel a été modifié par le : *Rectificatif au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des*.

²⁴ Gérard Hass, *Guide juridique du RGPD*, Édition ENI, avril 2018, JOUE L127 du 23/05/2018.

droit à l'information et corrélativement le droit à la vie privée et le droit de la protection des données personnelles. En outre, le travail de certaines personnes dans l'apanage numérique : c'est que l'effacement pur et simple des données semble techniquement extrêmement compliqué à faire une demande²⁵. En fait, d'un point de vue informatique, cela va à l'encontre même de la nature de l'appareil, il est déjà difficile de supprimer définitivement des données d'un ordinateur. Ainsi, quand l'information est rendue publique, chaque internaute peut faire des copies qu'il peut distribuer et propager. En réalité, dans le monde numérique, même si chacun des acteurs était de bonne foi et prêt à effacer un fichier numérique, encore faut-il pouvoir retrouver tous les liens, le stockage sur le Cloud numérique et dans les mémoires des ordinateurs incluant les serveurs. Conséquemment, cela devient mission impossible²⁶.

D'un point de vue pratique, le déréférencement ou la désindexation des pages concernées seraient la solution pragmatique et la plus facilement réalisable sur le plan technique²⁷. Pour plus de précisions, le déréférencement consiste à supprimer l'affiliation d'une personne physique avec des données personnelles la concernant, référencées sur les moteurs de recherche. Les données ne sont pas supprimées, mais leur lien avec l'entité concernée est effacé. Elles n'apparaissent donc plus dans les résultats d'une requête se basant sur l'identité de la personne physique à l'origine de la demande de déréférencement.

Le déréférencement, en opposition au référencement, est une pratique consistant à désindexer certaines données sensibles des moteurs de recherche. Ce procédé peut concerner une personne physique et intervient seulement si cette dernière en fait la demande.

²⁵ Yan Claeysen, « Oublions le 'droit à l'oubli' numérique »! La tribune (France) no 4465, 6 mai 2010, à la p 16.

²⁶ De Terwangne, *supra* note 16 ; Koops, *supra* note 18.

²⁷ Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD), *supra* note 7.

Le déréférencement est un droit reconnu et approuvé par la Cour de justice de l'Union européenne (CJUE) en 2014²⁸.

En conséquence de ce qui précède, le déréférencement reste la solution la plus adaptée puisque la plupart du temps lorsqu'une personne effectue une recherche sur Internet, elle se contente habituellement des sites proposés sur les premières pages de recherche. Ainsi, si les informations sensibles deviennent inatteignables par la suppression de la liste de résultats des liens, le problème est désormais pratiquement résolu. Néanmoins, les données ne sont pas pour autant supprimées, mais difficilement accessibles²⁹.

À cause de ces ambiguïtés et des différentes propositions de définition, les acteurs débattant du droit à l'oubli numérique, juriste ou non ne réussissent pas à s'entendre sur une définition claire. De surcroît, les données numériques concernées par le droit à l'oubli restent en ce moment très discutées.

Même s'il souffre de son appellation, le droit à l'oubli ou le droit d'être oublié se contraint comme un droit subjectif inhérent au droit à la vie privée. Il s'agit dans les faits d'une reconnaissance des principes de justice fondamentale³⁰ sous la forme de droit au respect de la vie privée, ce qui inclut le respect de la vie passée, « l'oubli » de ce que l'on voudrait faire disparaître sur Internet. Il est donc nécessaire d'inclure la notion « numérique » pour concrétiser ce que l'on souhaite définir comme le « droit à l'oubli » dans la présente étude³¹. En tant que personne et de société, nous avons la capacité de nous souvenir et d'oublier. La mémoire est notre capacité de stocker et de rappeler des informations

²⁸ *Ibid.*

²⁹ Dreyfus, *supra* note 10.

³⁰ Article 12, Déclaration universelle des droits de l'homme, adoptée par l'Assemblée générale des Nations Unies, le 10 décembre 1948. Voir Déclaration universelle des droits de l'homme, Rés AG 217A (III), Doc off AGNU, 3è sess, supp n°13, Doc NU A/810 (1948) 71. Voir également l'article 35 du Code Civil du Québec : « toute personne a droit au respect de sa réputation et de sa vie privée. Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise »; Code civil du Québec, RLRQ c CCQ-1991. Karim Benyechlef, Pierre-Luc Déziel, *le droit à la vie privée en droit québécois et canadien*, Montréal, Éditions Yvon Blais, 2018, aux p. 14, 37, 53, 85, 87, 94, 105, 129, 139, 151, 372, 409, 437.

³¹ Christian Charrière-Bournazel, « Propos autour d'Internet : l'histoire de l'oubli », *Gazette du palais* n° 11, Paris, (21 avril 2011) à la p 6.

appries. La mémoire, au fond, n'est rien d'autre que la trace de nos souvenirs éphémères, il est en principe plus facile d'oublier que de se rappeler.³² La technologie numérique a changé cela. De notre temps, avec un stockage de données illimitées et abordables, une exfiltration sans difficulté et un accès planétaire, la mémoire est devenue la norme pour toute personne et la société collectivement³³. Enfin, grâce aux réseaux numériques, l'Internet en particulier, nous pouvons accéder à ces accumulations d'informations sans fin, dans le monde entier à partir de nos ordinateurs personnels et nos téléphones portables³⁴. Dans cet environnement et en absence d'aucune autre considération, les données numériques sont ainsi conservées sans jamais être supprimées. C'est le point central du droit à l'oubli. Dans notre passé analogique, la valeur par défaut était de se débarrasser plutôt que de préserver. Désormais, la valeur par défaut est de conserver.

Les moteurs de recherche et les plateformes numériques préservent toutes les données de contenus accumulés et conservent chacune de nos requêtes de recherche, archivent les pages Web longtemps après les avoir mises hors ligne³⁵. Avec l'avènement de l'Internet et les moyens technologiques, une voie plus complète de nos actions seront recueillies plus que jamais et à tout jamais. Vivre dans un monde dans lequel nos vies sont enregistrées et les enregistrements sont conservés pour un temps indéfini, dans lequel l'oubli sociétal a été remplacé par un souvenir limpide, va assurément influencer notre perception de notre monde et comment se comporter dans celui-ci.

Si tout ce que nous faisons peut-être retenu contre nous des années plus tard, si tous les commentaires impulsifs sont préservés, ils peuvent facilement être combinés dans une

³² Helena D'Elia et Nathalie Dollez, *Exil et violence politique, les paradoxes de l'oubli*, Toulouse, Éres, 2019 aux pp 17 et 55 : « On ne décide pas d'effacer une mémoire ». C'est elle qui se structure avec l'oubli et qui, avec l'oubli, décide des rémanences. Celui qui ne pourrait oublier se retrouverait aussi désemparé que celui qui oublierait tout ».

³³ Nicolas Negroponte, *Being Digital*, New York, Vintage Books, 1996.

³⁴ Manuel Castells, *The Internet Galaxy*, Oxford, Oxford University Press, 2001.

³⁵ Cela a été découvert lorsque le gouvernement américain a assigné les moteurs de recherche à comparaître pour la recherche de données ; voir Katie Hafner et Matt Richtel, *Google résiste à l'assignation américaine des données de recherche*, New York Times, 20 janvier 2006, en ligne : <https://www.nytimes.com/2006/01/20/technology/google-resists-us-subpoena-of-search-data.html> (consulté le 15 août 2022).

image composite de nous-mêmes. S’effrayer de voir comment nos paroles et nos actions peuvent être perçues des années plus tard et sorties de leur contexte en l’absence d’oubli peut nous inciter à modifier notre comportement et notre liberté de parole³⁶. Indépendamment des autres préoccupations que nous pouvons avoir, il est difficile d’imaginer qu’un monde aussi inflexible et irréductible pourrait nous offrir la société libre et démocratique à laquelle nous sommes accoutumés à présent.

1.3 Genèse du droit à l’oubli numérique

Le « droit à l’oubli » est un concept juridique qui semble être relativement nouveau, revendiqué principalement vers le dernier tiers du XX^e siècle, et concrétisé à la fin des années 90, le droit à l’oubli devient au début du XXI^e siècle, un des avatars des libertés individuelles en relation avec le droit spécifique à la protection des données personnelles, cette revendication est à replacer dans un contexte d’affrontement social pour le droit de la protection de la vie privée et les nouvelles technologies numériques. En effet, il faut être en mesure de se souvenir de tout, ou quasiment, pour réclamer un véritable droit à l’oubli. Force est de constater également que les traces du passé sont étonnamment prégnantes pour demander la consécration d’un authentique droit à l’oubli³⁷.

³⁶ Françoise Blanchette et Deborah Johnson, *Data Retention and the Panoptic Society: The social Benefits of Forgetfulness*, manuscript, en ligne : https://www.researchgate.net/publication/220175071_Data_Retention_and_the_Panoptic_Society_The_Social_Benefits_of_Forgetfulness (consulté le 15 août 2022). Voir Oscar Grandy qui a décrit les structures de notre société panoptique dans Oscar Grandy, *The Panoptic Sort : A Political Economy of Personal Information* (1993) ; Voir aussi Michel Foucault qui a revisité l’idée de prison panoptique de Jeremy Bentham : Michel Foucault, *Discipline & Punish : The Birth of the Prison* (1995).

³⁷ Duton et Becht, *supra* note 4 ; Ausloos, *supra* note 4 à la p 9.

Le résumé de l’article de Jeff Ausloos vous donne une vue d’ensemble de la thèse de l’auteur. Au cours des dernières années, il y a eu beaucoup de bruit autour d’un soi-disant « droit à l’oubli ». Surtout en Europe, ce slogan est fortement débattu dans les médias, devant les tribunaux et par les régulateurs. Puisqu’une définition claire n’a pas (encore) émergé, l’article suivant tentera de lever le voile sur ce concept flou. La première partie va peser le pour et le contre de la droite les uns contre les autres. Il apparaîtra que le « droit à l’oubli » a clairement du mérite, mais qu’il doit être mieux défini pour éviter toute conséquence négative. En tant que tel, le droit n’est rien d’autre qu’un moyen de (re)donner aux individus le contrôle de leurs données personnelles et de rendre plus efficace le régime de consentement. La deuxième partie évaluera ensuite la mise en œuvre potentielle du droit. Des mesures sont requises au niveau normatif, économique, technique, ainsi que législatif. L’article conclut en proposant un « droit à l’oubli » limité aux situations de traitement de données où l’individu a donné son consentement. Combiné à une exception d’intérêt général, cela devrait

Dans les faits, l'action par une personne de demander la suppression d'informations la concernant, lorsqu'elles ne sont plus nécessaires à des fins légitimes, ne date pas des toutes dernières années. Effectivement, le concept d'oubli assimilé à l'amnistie a depuis longtemps servi à faire gracier des faits du passé pour conserver une certaine cohésion sociale et la paix civile, en imposant le silence sur une crise qui a agité la société³⁸. Par exemple, l'amnistie décrétée par les États rendant impossibles certaines poursuites peut aussi, dans certaines circonstances, annuler une sanction ou une peine associée à un crime. Le fondement de l'amnistie est le pardon d'un fait déterminé qui devient en fait impossible à une personne étant donné qu'il est censé ne s'être jamais produit. Mais encore, le fondement de l'amnistie est assurément le pardon d'un fait ou d'une action précise³⁹.

Le droit à l'oubli est reconnu depuis très longtemps par les tribunaux européens. Dès 1867, dans une cause célèbre, Alexandre Dumas (l'auteur français des *Trois Mousquetaires* et du *Comte de Monte-Cristo*) a eu gain de cause contre un photographe qui avait publié une série de photos intimes et dommageables d'Alexandre Dumas avec l'une de ses maîtresses. Au terme du procès, la Cour ordonna le retrait desdites photos en raison du principe que la vie privée de monsieur Dumas prévalait sur le droit de propriété du photographe et donc que ce dernier devait céder ses droits sur les photographies à monsieur Dumas⁴⁰.

(partiellement) rétablir l'équilibre des pouvoirs et permettre aux individus un contrôle plus efficace sur leurs données personnelles.

³⁸ De Terwangne, *supra* note 16 ; Voir aussi Roseline Letteron, « Le droit à l'oubli » (1996) 385 RDP 391.

³⁹ Par exemple, le pardon absolu se définit de la façon suivante au Canada : « Un pardon absolu est absolu et inconditionnel. Une personne qui bénéficie d'un pardon absolu est réputée n'avoir jamais commis l'infraction. Toutes les conséquences de la condamnation, telles une amende, une interdiction ou une confiscation, sont annulées dès l'octroi du pardon absolu. De plus, toute mention de la condamnation est effacée des dossiers de la police et des tribunaux, ainsi que de toutes les banques de données officielles. Le pardon absolu peut être une reconnaissance formelle qu'une personne a été condamnée à tort pour une infraction. Il peut également être accordé dans des cas exceptionnels où des considérations de justice, d'humanité et de compassion justifient l'octroi d'un pardon qui est absolu et sans condition.

en ligne : <<https://www.canada.ca/fr/commission-liberations-conditionnelles.html>> (consulté le 15 août 2022).

⁴⁰ Dumas se fait photographier avec sa dernière (Adah Isaacs Menken) sur ses genoux. Cette photo du vieil écrivain embrassé par l'une de ses maîtresses provoque un scandale et lui ferme les portes de l'Académie française. Voir Biographie d'Alexandre Dumas, en ligne : < www.alalettre.com/dumas-bio.php>.

Le droit à l'oubli dans la presse est aussi une histoire ancienne, selon la doctrine, l'expression première est attribuée à Gérard Lyon-Caen qui l'aurait utilisée en 1966 dans ses commentaires écrits concernant une action en justice de l'ancienne maîtresse de Landru, un célèbre tueur en série et criminel français⁴¹, Mme Fernande Segret. Cette dernière demande réparation du préjudice allégué découlant de la sortie d'un film par le cinéaste Claude Chabrol basé sur la biographie de son amant⁴². Par la suite, le Tribunal de grande instance (TGI) de Paris utilise directement la notion du droit à l'oubli en 1983, la Cour affirme en ces mots : « toute personne qui a été mêlée à des événements publics peut, le temps passant, revendiquer le droit à l'oubli ». Elle ajoute que « le rappel de ces événements et du rôle qu'elle a pu y jouer est illégitime, s'il n'est pas fondé sur les nécessités de l'histoire ou s'il peut être de nature à blesser sa sensibilité » et que « ce droit à l'oubli qui s'impose à tous, y compris aux journalistes, doit également profiter à tous, y compris aux condamnés qui ont payé leur dette à la société et tentent de s'y réinsérer »⁴³.

Le droit à l'oubli a conséquemment intégré le droit actuel ou positif, il y a déjà plusieurs années par la voie de la responsabilité civile, depuis, cette locution juridique a fait Florès chez les juristes, les informaticiens comme les profanes. En poursuivant dans la même direction, le droit à l'oubli n'est pas sans rappeler d'autres droits aux noms atypiques et souffrant d'une certaine imprécision comme le droit à l'autonomie personnelle, le droit à l'autodétermination, le droit au respect de son honneur et à la reconnaissance de sa dignité

⁴¹ Gérard Lyon-Caen, né le 4 octobre 1919 à Paris et mort dans cette même ville le 13 avril 2004, est un juriste français. Professeur en droit social, il est considéré comme l'un des plus grands spécialistes français de sa discipline ; en ligne : <<https://www.universalis.fr/encyclopedie/gerard-lyon-caen/>> (consulté le 15 août 2022).

⁴² L'affaire « Landru », en 1965. À l'époque, l'ancienne maîtresse du célèbre criminel demandait, devant le juge civil, réparation du préjudice que lui causait la sortie d'un film de Claude Chabrol relatant une période de sa vie, qu'elle aurait préféré enfouir dans le passé. Le juge a alors évoqué une « *prescription du silence* », pour finalement rejeter la demande au motif que la requérante avait elle-même publié ses mémoires et que le film reprenait des faits relatés dans des chroniques judiciaires parfaitement accessibles. Voir : Mme S. c. Soc. Rome Paris Film? JCP 1966 I 14482, n. Lyon-Caen TGI Seine, 14 octobre 1965. Ce jugement a été confirmé en appel : CA Paris 15 mars 1967.

⁴³ M.c. Fillipacchi et Cogedipresse, JCP 1983kk, II, 20434, TGI Paris, 20 avril 1983; note R. Lindon.

ou encore le droit au bonheur, au bien-être et le droit à l'anonymat, etc. Comme nous l'avons déjà évoqué, la définition même du droit à l'oubli semble problématique pour certains, comme la professeur Roseline Letteron qui interprète l'oubli comme une singularité psychologique et biologique qui ne concerne en rien le juriste « perte d'un souvenir », il ne peut être appréhendé de manière substantielle par le droit pour lequel il restera toujours une fiction. Si une norme juridique peut imposer le silence, elle ne peut en aucun cas imposer l'oubli⁴⁴. Plus près de nous, le professeur de droit Pierre Trudel s'exprime de la manière suivante sur le sujet :

Dans les systèmes juridiques d'inspiration civilisée, l'oubli se présente comme un droit indirect. Il découle du droit à la vie privée ou même du droit à la réputation. L'oubli présuppose une information ayant déjà circulé dans un espace collectif. L'oubli a pour objet de l'information qui n'est pas secrète, qui a déjà été portée à la connaissance d'une ou de plusieurs personnes⁴⁵.

Un peu plus loin, le professeur Trudel continue :

Dans le droit civil d'inspiration française, la notion de faute a constitué le Vecteur par lequel fut déduite une obligation d'oublier. Lorsque le rappel d'une information est jugé fautif, celui qui s'y livre sera tenu d'indemniser la personne qui en a subi un préjudice⁴⁶.

Toujours selon cet auteur :

En s'appuyant sur ce principe à caractère universel, les tribunaux ont considéré qu'en certaines circonstances, on peut commettre une faute de violation d'oubli. De ce constat, certains auteurs ont déduit l'existence d'un droit à l'oubli⁴⁷. À ce titre, l'auteur nous dirige vers des exemples

⁴⁴ Letteron *supra* note 38 aux pp 385-386.

⁴⁵ Pierre Trudel, « L'oubli en tant que droit et obligation dans les systèmes juridiques civilistes », Texte inédit préparé pour le cours de droit du cyberspace, Faculté de droit, Université de Montréal, 2013, (8 septembre 2016) en ligne : <<https://pierretrudel.openum.ca/publications/pierre-trudel-loubli-en-tant-que-droit-et-obligation-dans-les-systemes-juridiques-civilistes>> à la p 1.

⁴⁶ *Ibid.*

⁴⁷ *Ibid.*

tirés de la jurisprudence québécoise qui remonte à 1889 dans lequel la Cour supérieure du Québec a reconnu un droit à l'oubli dans l'affaire *Goyette c. Rodier*⁴⁸. Le juge a estimé que le journal le Violon avait eu tort de faire revivre certaines accusations depuis longtemps oubliées concernant Odilon Goyette. Ce fut confirmé en appel⁴⁹.

L'auteur Pierre Trudel nous donne plusieurs exemples de jurisprudence semblable plus récente et conclut ainsi :

Ainsi envisagé, l'oubli dans les systèmes civilistes se présente comme un droit de l'individu d'exercer un contrôle à l'égard d'informations déjà existantes portant sur un événement passé. Il ne peut avoir une portée universelle. Son étendue et sa consistance découlent forcément d'un constat à l'égard de l'existence d'un intérêt public à la redivulcation de l'information. L'oubli est une obligation et un droit dans la mesure où l'information visée porte sur une personne, que l'information ne répondra pas à l'intérêt public⁵⁰.

Obligé de constater que même en droit québécois, le droit à l'oubli a une résonance lointaine.

1.4 Résolution 73(22) de 1973

Poussons notre incursion historique de ce droit, en septembre 1973, le Conseil de l'Europe adopte la résolution 73(22)⁵¹, relativement « à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé » laquelle résolution prévoit pour la toute première fois aux gouvernements des États membres une série de recommandations pour prévenir les abus lors de l'enregistrement du traitement et

⁴⁸ *Goyette c. Rodier* (1889) 20 R.L. 108, 110 (C. Rev).

⁴⁹ Trudel, *supra* note 45 à la p 2.

⁵⁰ *Ibid* à la p. 5.

⁵¹ Conseil de l'Europe, Comité des ministres, 224^{ème} réunion des délégués des ministres, Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, Annuaire européen 1973, 26 septembre 1973. Le conseil de l'Europe est une organisation intergouvernementale instituée le 5 mai 1949 par le Traité de Londres. Il comprend 41 États membres, dont 27 sont membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et la primauté du droit. Celle-ci a été adoptée en 1950 et est entrée en vigueur en 1953. Voir Convention Européenne des droits de l'homme, (21 juillet 2022) en ligne <<https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=fr>>

de la diffusion d'informations à caractère personnel par l'ensemble structuré des banques de données électroniques privées.

Comme on peut le lire à l'annexe de la résolution (73)22 à son article 4 qui stipule « des règles devront être établies pour déterminer la période au-delà de laquelle certaines catégories d'informations ne pourront plus être conservées ou utilisées »⁵². Obligé de constater que le Conseil de l'Europe prévoyait déjà une date de péremption pour la suppression de certaines informations qui ne pourront plus être conservées ou utilisées. De plus, la même résolution prévoit aussi que certaines informations ne peuvent être utilisées à d'autres fins que celles pour lesquelles elles ont été enregistrées ni communiquées à des tiers sans l'autorisation appropriée⁵³. La même résolution précise à son article 7 : « toute diligence doit être faite pour corriger les informations inexactes et pour effacer les informations périmées ou obtenues de façon illicite⁵⁴ ». D'ores et déjà, on peut y voir la volonté législative européenne d'encadrer les données électroniques. La résolution (73)22 fut la base des principes juridiques à l'égard de la protection des données à caractère privé en Europe, pavant ainsi une ère de législation en exerçant un certain contrôle des données informatiques, notamment en France, via la Loi no 78-17 de janvier 1978, relativement à l'informatique, aux fichiers et aux libertés⁵⁵. Cette Loi prévoit entre autres la création d'une Commission nationale de l'informatique et des libertés, cette autorité administrative indépendante dispose d'un pouvoir de contrôle et de sanction. Elle a pour mission de veiller à ce que le développement des nouvelles technologies ne porte atteinte ni l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques⁵⁶. La Commission nationale de l'information et des libertés (CNIL) est donc informée de la finalité de la collecte et la conservation des informations. En conséquence

⁵² Résolution (73) 22, *supra* note 51 à l'article 4 de l'annexe.

⁵³ *Ibid* article 5 de l'annexe.

⁵⁴ *Ibid* article 7 de l'annexe.

⁵⁵ « Informations inexactes et pour effacer les informations périmées ou obtenues de façon illicite ». Voir la Loi No 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (plus connue sous le nom de « Loi informatique et libertés ») qui est une loi française qui régleme la liberté de traitement des données personnelles. Elle est disponible sur Légifrance, (21 juillet 2022) en ligne : <<https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/>>

⁵⁶ *Ibid*.

de l'application de la loi, lorsque ces finalités disparaissent, les données ainsi conservées doivent être détruites⁵⁷. Elles sont pour ainsi dire « oubliées » et la CNIL garantit la conformité de ces formalités procédurales. Dès lors, le droit à l'oubli devient « numérique » et présente la particularité d'être la conséquence du principe de la prédestination des assises juridiques du droit à l'oubli numérique.

1.5 La Directive 95/46/CE

D'autres textes législatifs ont suivi particulièrement au niveau européen. C'est en l'occurrence le cas dans la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre, 1995⁵⁸. La Directive 95/46/CE, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Comme son nom officiel l'indique, la direction cible l'harmonisation des normes juridiques des différents États membres de l'Union européenne en matière de protection des données personnelles.

Afin d'harmoniser la protection des données personnelles et faciliter leur échange à travers les frontières, l'OCDE avait publié, en 1980, des « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel ». Sans valeur contraignante, ces lignes directrices, qui n'ont jamais été mises en œuvre par les États-Unis, ont inspiré la Directive 95/46/CE. Les sept principes y figurant ayant été repris : principe de la limitation en matière de collecte ; de la qualité des données ; de la limitation de l'utilisation ; des garanties de sécurité ; de la participation individuelle et de la responsabilité⁵⁹.

⁵⁷ *Ibid* article 22.

⁵⁸ CE, *Directive (CE) 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, [1995] JOUE L 281, 23 novembre 1995 (ci-après la directive CE 95/46). Il s'agit d'une ancienne directive de l'Union européenne abrogée le 25 mai 2018 et qui constituait le texte de référence en matière de protection des données à caractère personnel. Elle est disponible en ligne (21 juillet 2022) sur Légifrance : <<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000697074>>

⁵⁹ *Ibid* articles 2, 4, 12 et 14. Voir également les sept principes relatifs aux données à caractère personnel de l'Organisation de la Coopération et du développement économique (OCDE) que sont :

- Les personnes dont les données personnelles sont collectées doivent en être avisées.

En substance, les données personnelles ne doivent pas être soumises à un traitement automatisé, sauf si celui-ci remplit les exigences fondées sur trois principes : proportionnalité, transparence et finalité légitime. La directive reprend essentiellement les principes généraux et les droits imposés dans la Loi informatique et libertés de 1978⁶⁰ et qui forment un cadre législatif général de la protection des données informatiques personnelles.

Corollairement au développement de l'Internet des années 90, l'Union européenne se dotait d'instruments juridiques pour répondre aux nouveaux défis en relation avec ce phénomène technologique sans précédent. En effet, avec l'arrivée de la numérisation, émerge une interpellation représentative et revendique de celle du droit à l'oubli, qui au fil des années, s'est élargi inéluctablement à un « droit à l'oubli numérique ». En 2010, Viviane Reding, Vice-présidente de la Commission européenne et Commissaire européenne à la justice, aux droits fondamentaux et à la citoyenneté prononcent un discours lors d'une réunion de la « European Data Protection and Privacy Conference » où elle introduit clairement et sans équivoque le droit à l'oubli et la protection des données personnelles comme un droit fondamental qui fait partie des valeurs juridiques européennes⁶¹. Cette initiative de Viviane Reding aboutit le 25 janvier 2012 avec la publication par la Commission européenne d'une

-
- Ces personnes doivent être informées de l'identité des parties qui collectent leurs données.
 - Une fois collectées, les données personnelles doivent être conservées en lieu sûr et protégées contre tout risque d'utilisation abusive, de vol ou de perte.
 - Les données personnelles ne doivent pas être divulguées ni partagées avec des tiers sans le consentement des personnes concernées.
 - Les personnes concernées doivent avoir accès à leurs données personnelles et être autorisées à corriger toute inexactitude.
 - Les données collectées ne doivent pas être utilisées à des fins autres que celles qui ont été déterminées.
 - Il incombe aux responsables de la collecte des données personnelles d'assurer le respect de ces sept principes. Voir la Loi informatique et libertés, *supra* note 55.

⁶⁰ Loi informatique et libertés, *supra* note 55.

⁶¹ Viviane Reding, "Privacy Matters-Why the EU Need New Personal Data Protection Rule", The European Data Protection and Privacy Conference, Brussels, 30 November 2010, en ligne : (21 juillet 2022) : <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_10_700/SPEECH_10_700_EN.pdf>

proposition de régulation européenne pour la protection des données et le droit à l’oubli qui est un des piliers de la réforme⁶².

Le texte est par la suite révisé et amendé par le Parlement européen et le Conseil des ministres. Il est voté le 12 mars 2014 par le Parlement européen. Ce nouveau cadre juridique se compose de deux propositions législatives :

- une proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données), et
- une proposition de directives du Parlement européen et du Conseil relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d’enquêtes et de poursuites en la matière, ou d’exécution de sanctions pénales et à la libre circulation de ces données⁶³.

Également, il est important de souligner que les règles de l’Union européenne s’appliquent même si le traitement des données personnelles se fait « à l’étranger par des entreprises implantées sur le marché européen et proposant leurs services aux citoyens de l’Union »⁶⁴.

Comme nous avons vu précédemment, la pièce maîtresse de la législation de l’Union européenne en matière de protection des données à caractère personnel, à savoir la Directive 95/46/CE, avait été adoptée en 1995 avec deux objectifs à l’esprit : protéger le droit fondamental à la protection des données et garantir la libre circulation des données à caractère personnel entre les États membres. Elle a été complétée par la décision-cadre

⁶² European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World”, A European Data Protection Framework for the 21st Century, Brussels, 25.1.2012 COM (2012) 9 final, en ligne (21 juillet 2022) : <<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF>>

⁶³ *Ibid.*

⁶⁴ *Ibid.*

2008/977/JAI destinée, à titre d'instrument général, au niveau de l'Union, à protéger les données à caractère personnel dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale⁶⁵.

Le Parlement européen a dû adapter sa législation pour la protection des données à caractère personnel considérant l'évolution fulgurante des technologies numériques. En effet, il est facile de constater que la rapide évolution des technologies a créé de nouveaux enjeux juridiques pour la protection des données. Le partage et la collecte de données ont connu une augmentation spectaculaire. Le Parlement européen fait le bilan des dernières années pour conclure aux vulnérabilités des États membres face à l'accumulation incessante des données permettant tant aux entreprises privées qu'aux pouvoirs publics d'utiliser ces données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus de personnes physiques rendent des informations les concernant accessibles à tout un chacun, où qu'il se trouve dans le monde. Les nouvelles technologies ont ainsi transformé l'économie et les rapports sociaux.

1.6 Charte française sur le droit à l'oubli 2010

Dans ce même ordre d'idée, le 13 octobre 2010 à Paris, une dizaine de signataires réunis par Nathalie Kosciusko-Morizet, Secrétaire d'État chargée de la prospective et du développement de l'économie numérique pour le gouvernement français, ont adopté une Charte consacrée au droit à l'oubli numérique. En fait, deux Chartes ont été signées en 2010. La première la Charte du droit à l'oubli numérique⁶⁶ vise principalement les moteurs de recherche et les représentants de site collaboratif et signataires à mettre en place de

⁶⁵ La directive CE 95/46, *supra* note 58 à la p 31. Voir aussi la Décision-cadre 2008/977/JI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, à la p 60, (ci-après « la décision-cadre »).

⁶⁶ Portail du Gouvernement, « Charte du droit à l'oubli numérique : mieux protéger les données personnelles des internautes », sur le monde. Fr. 13 octobre 2010, en ligne : <http://www.gouvernement.fr/node73763>. Voir aussi Comment mieux protéger les données publiées intentionnellement par les internautes ? Une charte a été signée, mercredi 13 octobre, sous l'égide de Nathalie Kosciusko-Morizet, par les sites collaboratifs (principalement les réseaux sociaux, blogs et forums) et les moteurs de recherche. Elle garantit le respect de la vie privée des internautes; en ligne : <http://www.gouvernement.fr/gouvernement/charte-du-droit-a-l-oubli-numerique-mieux-protoger-les-donnes-personnelles-des-interna> Créé 2010-10-18 08 :08.

nouveaux dispositifs afin de garantir la protection des données privées des utilisateurs et de prévoir de nouveaux dispositifs numériques pour permettre la suppression ou et la désindexation des informations nuisibles à la réputation des personnes. Une manière de faire disparaître les résultats des moteurs de recherche sur les données à la demande, simplement et rapidement. Nathalie Kosciusko-Morizet fait remarquer que : « Il ne faut pas diaboliser Internet, il y a de nombreux contenus mis en ligne que nous voulons garder, mais dans certains cas, nous aimerions pouvoir les effacer »⁶⁷.

La deuxième, Charte signée le 30 septembre de la même année, Charte du droit à l'oubli numérique dans la publicité ciblée, l'objectif est de traiter les données personnelles collectées passivement sans que les utilisateurs de l'Internet en aient vraiment conscience⁶⁸.

Les Chartes sont une des actions du gouvernement français du concept plus général du droit à l'oubli. Toutefois, il faut préciser que ces Chartes ne sont pas contraignantes et que leurs adhésions sont purement volontaires. D'ailleurs, ni Google et ni Facebook font partie de la liste des signataires⁶⁹. Les documents des Chartes expliquent que les assises des principes se retrouvent à la protection de la vie privée de la personne garantie au sein de l'Union européenne⁷⁰.

⁶⁷ Kosciusko-Morizet *supra* note 66.

⁶⁸ Alexandre Laurent, « Publicité en ligne : une charte pour 'droit à l'oubli' » (1^{er} juin 2018), en ligne (blogue) : Alexandre Laurent : <<https://www.clubic.com/pro/webmarketing/publicite-en-ligne/actualite-369842-publicite-ligne-charte-droit-oubli.html>>. Selon lui, « La publicité ciblée, c'est ce concept selon lequel on va profiter de votre historique de navigation, de vos préférences, des recherches effectuées sur les moteurs ou de votre position géographique pour affiner le message publicitaire qui vous est adressé, en partant du principe que plus fin aura été le ciblage plus rapidement vous succomberez ».

⁶⁹ Laurent Checola, « 'Droit à l'oubli' sur Internet : une charte signée sans Google ni Facebook, » Le Monde.fr (13 octobre 2010), en ligne : <https://www.lemonde.fr/technologies/article/2010/10/13/droit-a-l-oubli-sur-internet-une-charte-signee-sans-google-ni-facebook_1425667_651865.html>. Voir aussi Christophe Lagane, « Google et Facebook oublient la charte du droit à l'oubli numérique », Silicon.fr. (14 octobre 2010), en ligne : <<https://www.silicon.fr/google-et-facebook-oublent-la-charte-du-droit-a-loubli-numerique-42481.html>>

⁷⁰ Checola *supra* note 69 à la p 2.

1.7 Le Règlement européen 2016/679

Nous avons révélé précédemment que la Directive 95/46/CE (Règlement général sur la protection des données)⁷¹ constituait le texte de référence en matière de protection des données aux attributs personnels et particulièrement pour l'évolution du droit à l'oubli numérique. Alors, le Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abroge la Directive 95/46/CE du Règlement général, pour la remplacer par le Règlement (UE) 2016/679 du Parlement européen et Conseil⁷². Le Règlement général sur la protection des données ou RDPG est le nouveau texte législatif de référence au sein de l'Union européenne qui régit le traitement et l'utilisation des données à caractère personnel⁷³. Ce règlement est entré en vigueur le 25 mai 2018 sous le numéro 2016/679 et reprenant les grandes lignes de la Directive 95/46/CE et du texte, de la Loi française sur l'informatique et la liberté du 6 janvier 1978⁷⁴. En substance, ce dispositif juridique prévoit des droits clairs à tout citoyen européen pour leur procurer un certain contrôle sur leurs données parmi lesquels on retrouve notamment le « droit à l'oubli » et/ou le « droit à l'effacement » des données personnelles en toutes lettres⁷⁵.

⁷¹ La directive CE 95/46, *supra* note 58.

⁷² Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Il a été modifié par le: *Rectificatif au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE (règlement général sur la protection des données) JOUE L127 2 du 23/05/2018.*

⁷³ *Ibid.*

⁷⁴ Loi informatique et libertés, *supra* note 55 et note 58.

⁷⁵ Règlement (UE) 2016/679, *supra* note 72. Il est prévu par l'article 17 Chapitre III, du Règlement général sur la protection des données, (RGPD).

Il est important de signaler que le Règlement (UE) 2016/679 du Parlement européen et du Conseil⁷⁶ dans son préambule expose l'importance et les principes juridiques supérieurs qui auréolent le traitement des données personnelles de la manière suivante :

Considérant ce qui suit : La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée « Charte ») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant⁷⁷.

Le Parlement européen et du Conseil précise un peu plus loin dans ce même préambule certaines limites : le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément aux principes de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrée par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial et la diversité culturelle, religieuse et linguistique, etc.⁷⁸

⁷⁶ *Ibid.*

⁷⁷ *Ibid*, préambule article (1) : « Le traitement des données à caractère personnel est un droit fondamental ».

Cet article a été fondé sur l'article 286 du traité instituant la Communauté européenne et sur la directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p.31), ainsi que sur l'article 8 de la CEDH et sur la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, ratifiée par tous les États membres. L'article 286 du traité CE est désormais remplacé par l'article 16 du traité sur le fonctionnement de l'Union européenne et l'article 39 du traité sur l'Union européenne. Il convient de noter également le règlement (CE) no 45/2001 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, en ligne : <https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex%3A32001R0045> (consulté le 15 août 2022).

⁷⁸ Règlement (UE) 2016/679, *supra* note 72. Voir l'article 4 du préambule.

Considérant que le Règlement général sur la protection des données à caractère personnel (2016/679) constitue le texte de référence en la matière, on doit retenir que le traitement des données est un droit fondamental et que ce droit n'est pas absolu.

Le droit à l'oubli numérique prévu par l'article 17 du RGPD⁷⁹ et également connu sous le nom du droit à l'effacement des données a pour objectif de permettre légitimement et sans ambiguïté à toute personne résidant dans un pays membre de l'Union européenne de demander à l'organisme prévu à cet effet d'effacer les données à caractère personnel qui lui « appartient »⁸⁰ ou plutôt qui la concerne⁸¹.

Dans le cadre de l'analyse du droit à l'oubli numérique selon le RGPD, il est fondamental de faire l'examen des quatre principes clés du RGPD pour une meilleure compréhension des outils juridiques sous-jacents aux mécanismes d'application pour le retrait des données à caractère personnel.

Le RGPD précise que le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant.

Le RGPD repose sur le principe de la transparence des entreprises vis-à-vis des utilisateurs. Le Règlement propose donc que, l'utilisation des données personnelles de vos clients et

⁷⁹ *Ibid* au Chapitre III, article 17.

⁸⁰ À qui appartient nos données personnelles ? Primo une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable selon la CNIL. Voir : CNIL, données personnelles, en ligne : <<https://www.cnil.fr/fr/definition/donnee-personnelle>> (consulté le 15 août 2022).

Secondo, selon Alice Vitard, journaliste, informaticienne, « [d]un point de vue juridique, il n'existe aucun droit de propriété sur les données personnelles. Pour certains, il serait indispensable de consacrer une telle prérogative pour réguler l'environnement numérique et redonner le pouvoir aux citoyens. Pourtant, cette solution nie complètement le rapport de force qu'il existe entre géants technologiques et utilisateurs ». Alice Vitard, « Les données personnelles appartiennent-elles aux utilisateurs ? » L'Usine Digitale, (29 octobre 2019), en ligne : <<https://www.usine-digitale.fr/editorial/les-donnees-personnelles-appartiennent-elles-aux-utilisateurs.N898729>>. Voir également Règlement (UE) 2016/679, *supra* note 72, Chapitre III, articles 12 à 17.

⁸¹ Règlement (UE) 2016/679, *supra* note 72, Chapitre III article 12.

prospects demeure permise, mais il devient obligatoire d'informer les personnes concernées de l'usage qui sera fait de leurs informations.

Avec l'adoption du RGPD, les données personnelles n'appartiennent plus aux compagnies qui les collectent, mais demeurent la propriété des individus concernés. Ainsi, selon ce règlement européen, tout utilisateur doit pouvoir exercer les droits suivants :

- Accéder à ses données personnelles ;
- Savoir comment elles sont utilisées ;
- Demander que d'éventuelles erreurs soient corrigées ;
- Limiter le traitement des données ;
- Obtenir et réutiliser ses données personnelles ;
- Refuser certaines utilisations⁸² ;
- Demander le retrait des données (le droit à l'oubli)⁸³.

Enfin, le RGPD vise à responsabiliser les entreprises qui collectent et utilisent des données. Ces dernières doivent donc prendre les mesures nécessaires pour assurer la sécurité des informations personnelles des utilisateurs. Elles peuvent notamment utiliser des moyens physiques, comme des gardes de sécurité pour protéger les serveurs, ou des moyens technologiques comme en cryptant les données pour en assurer la protection⁸⁴.

1.8 Droit à l'effacement (droit à l'oubli)

En vertu de l'article 17 du RGPD, une personne concernée a « le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données

⁸² *Ibid* Chapitre III, articles 12 à 16.

⁸³ *Ibid* Chapitre III, article 17.

⁸⁴ *Ibid* Chapitre IV, articles 25 à 34.

à caractère personnel dans les meilleurs délais lorsque l'un des motifs suivants s'applique »⁸⁵ :

- Les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
- La personne concernée retire le consentement sur lequel est fondé le traitement ;
- La personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ;
- Les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- Les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
- Les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1⁸⁶.

Le responsable du traitement doit alors démontrer qu'il a accompli les opérations nécessaires pour donner suite à la demande de la personne concernée en conformité avec l'article 17 de RGPD alinéa 2 que nous citons :

Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci⁸⁷.

⁸⁵ *Ibid* Chapitre III, article 17.

⁸⁶ *Ibid*. Voir aussi Louis-Philippe Gratton, "The Latest Consolidated Version of the Regulation with Corrections by Corrigendum", OJ L 127, (23.5.2018) à la p 2 ((EU) 2016/679). Source : EUR-lex, en ligne : <<https://gdpr-text.com/wp-content/uploads/2020/06/gdpr-text.com-article-16-encommentary.pdf>>. Selon lui, le « right to be forgotten » was hailed as a breakthrough with the adoption of the General Data Protection Regulation, even though it existed in a limited form before. Article 17 provides for a broader « right to erasure », to take into account the exact wording of the provision. European Union residents have a right to as for the deletion of their personal data, and the organization that holds the data has a corresponding obligation to erase them « without undue delay » under a certain number of circumstances.

⁸⁷ Règlement (UE) 2016/679, *supra* note 72 Chapitre III, article 17 au para 2.

De plus, le responsable du traitement a à sa charge l'obligation de communiquer à chaque destinataire des données tout rectification, effacement ou limitation du traitement. Il peut toutefois se soustraire à cette obligation si le traitement des données se révèle impossible ou suppose un effort disproportionné. Le responsable doit fournir à la personne concernée les informations sur ces destinataires sur demande⁸⁸.

Le rejaillissement de l'application du RGPD sur la notion juridique du droit à l'oubli, qui en fait, encadre sa finalité, en écartant les éventuels dangers qu'une personne soit atteinte de manière durable par utilisation des données qui lui appartiennent ou qui la concernent à son insu. Également, il n'est pas important que lesdites données se retrouvent sur Internet par sa propre initiative, ou par celle d'une tierce personne. Le citoyen dans un pays de l'Union européenne obtient du responsable du traitement l'assurance de l'effacement des données ayant un caractère personnel. En supplément, le Règlement général sur la protection des données prévoit d'effacer la diffusion de ces données particulièrement quand la personne intéressée n'accorde plus son consentement pour leur utilisation.

Il en résulte, qui est également possible d'évoquer le droit à l'oubli numérique lorsqu'un contenu embarrassant pour la personne concernée des informations à effacer s'affiche sur les réseaux sociaux. Dans la même veine, la personne ne souhaite plus voir un référencement vers un lien gênant la concernant peut exiger, de l'opérateur du moteur de recherche ou autre plateforme numérique responsable du traitement des données de cesser le référencement associé, et ce, dans les meilleurs délais⁸⁹.

⁸⁸ *Ibid* Chapitre III article 19.

⁸⁹ *Ibid* Chapitre III article 16 et 17. Souvent, on distingue deux formes de ce même droit : Le droit au déréférencement et le droit à l'effacement l'article 17 du RGPD ne fait pas la différence dans l'application de son règlement au chapitre de la rectification et de l'effacement.

1.9 Le droit à l'oubli numérique n'est pas absolu

L'article 17 paragraphe 3 RGPD, présente quelques limites du droit à l'oubli numérique puisque le responsable du traitement n'est pas obligé exceptionnellement d'effacer les données dans la mesure où ce traitement est nécessaire :

- « a) à l'exercice du droit à la liberté d'expression et d'information ;

- b) pour respecter une obligation légale qui requiert le traitement prévu par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3 ;
- d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ; où
- e) à la constatation, à l'exercice ou à la défense de droits en justice⁹⁰ ».

Le Parlement européen et du Conseil par l'adoption de l'article 17, paragraphe 3 RGPD atteint un certain équilibre, en autres, l'exigence d'une mise en balance entre d'une part les droits fondamentaux au respect de la vie privée et la protection des données à caractère personnel, consacré par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne et d'autre part, le droit fondamental à la liberté d'information garantie par l'article II de la même Charte⁹¹.

⁹⁰ Règlement (UE) 2016/679, *supra* note 72, Chapitre III, article 17, paragraphe 3.

⁹¹ « Le droit à l'oubli n'est pas absolu (une balance doit être effectuée entre le droit à la vie privée du demandeur et le droit à l'information du public, l'arbitrage entre ces deux libertés fondamentales dépend de la nature des données personnelles ». CJUE, 6 décembre 2019, C-136/17.
Sur cette base, le Conseil d'État a, par 13 décisions rendues le 6 décembre 2019, apporté d'importantes précisions sur la mise en œuvre du droit au déréférencement. Le Conseil d'État indique que pour chaque

Comme on peut se rendre compte, le Parlement européen et le Conseil de l'Union européenne⁹² s'est doté d'instruments législatifs pour appréhender, de nouveaux défis pour le droit à la vie privée et les droits de la personne en général en réaction de la révolution numérique. Ce qui a eu comme effet l'émergence croissante d'une élucubration sur la nécessité de réfléchir à un nouveau droit, intimement lié à ce contexte numérique de rétention tous azimuts des données personnelles : le droit à l'oubli ou le droit à l'effacement numérique pour harmoniser le cyberspace et la vie privée. Force est de remarquer, cette harmonisation se dédouble en une conciliation entre libertés économiques créée par l'interconnexion mondiale et les droits fondamentaux⁹³. En effet, la collecte insatiable d'information est intrinsèquement liée à un modèle économique générant chaque année des revenus qui dépassent l'imagination⁹⁴. Considérant que les outils juridiques pour répondre à cette nouvelle réalité apparaissaient particulièrement inadaptés pour faire face à ces

demande de déréférencement, l'intérêt du public à avoir accès à cette information doit être mis en balance avec trois grandes catégories de critères :

- Les caractéristiques des données en cause : contenu des informations, leur date de mise en ligne, leur source, etc. ;
- La notoriété et la fonction de la personne concernée ;
- Les conditions d'accès à l'information en cause : la possibilité pour le public d'y accéder par d'autres recherches, le fait que l'information ait été manifestement rendue publique par la personne concernée, etc.

Si les informations publiées sont des données dites « sensibles » (religion, orientation sexuelle, santé, etc.), elles doivent faire l'objet d'une protection particulière et donc, dans la mise en balance, d'une pondération plus importante. Le déréférencement ne pourra être refusé que si ces informations sont « strictement nécessaires » à l'information du public. En revanche, si ces données ont été manifestement rendues publiques par la personne concernée, leur protection particulière disparaît.

Communiqué de presse du Conseil d'État du 6 décembre 2019, « Droit à l'oubli : le Conseil d'État donne le mode d'emploi », (6 décembre 2009) en ligne : <<https://www.conseil-etat.fr/actualites/droit-a-l-oubli-le-conseil-d-etat-donne-le-mode-d-emploi>>.

⁹² Le Parlement européen (PE) est le bras législatif de l'Union européenne (UE) et l'une de ses sept institutions. Il est composé de 705 membres (MPE) représentant l'ensemble des pays de l'UE. Le Parlement européen décide sur la législation de l'Union, y compris sur le budget pluriannuel, avec le Conseil de l'Union européenne (les ministres des États membres de l'Union). Les autres institutions, dont la Commission Européenne, rendent des comptes au Parlement. Les députés au Parlement européen sont élus dans les États membres de l'UE et représentent environ 446 millions d'habitants. Au fil des années et de modifications apportées aux traités européens, le Parlement a acquis des compétences législatives et budgétaires considérables. Voir la FAQ du service du porte-parole du Parlement : « Quelles sont les compétences et les procédures du parlement européen ? », (21 juillet 2022) en ligne : <<https://www.europarl.europa.eu/news/fr/faq/16/quelles-sont-les-competences-et-procedures-legislatives-du-parlement-europeen>>

⁹³ Sur les aspects conceptuels de cette notion, voir: D. Lochak et V. Champeil-Desplats, *Libertés économiques et Droits de l'Homme*, Presses Universitaires de Paris Ouest Nanterre la Défense, 2011.

⁹⁴ Jean Tillinac, « Le Web 2.0 ou l'avènement du client ouvrier » (2006) 60 :1 *Quaderni*, Aux pp.19-24.

enjeux urgents. Le Parlement européen a réagi par la consolidation de la législation en la matière. Comme nous l'avons déjà vu, le texte européen le plus complet et le plus large d'implémentation est ce qu'on qualifie la pierre angulaire du droit à l'oubli numérique est la Directive 95/46/CE⁹⁵.

En 1995, date d'une période où le Réseau mondial Internet n'en était qu'à ses balbutiements. Assurément, la question de la protection des données personnelles a été de longue date inscrite à l'agenda des institutions législatives européennes des dernières années. L'ensemble de ces efforts législatifs s'est en sus, doublé de la mise en œuvre d'une politique sociale cohérente en la matière. À ce titre, le travail de l'Union européenne par ses avis, directives et règlements a largement contribué à construire un cadre juridique et élaboré à même de parer aux enjeux de ce dédoublement : droits fondamentaux et Internet⁹⁶.

1.10 Charte des droits fondamentaux de l'Union européenne

L'un des facteurs contributifs d'évolution s'inscrit dans le cadre de l'adoption de la Charte des droits fondamentaux de l'Union européenne (UE) proclamée lors du Conseil européen de Nice, le 7 décembre 2000⁹⁷, publiée le 18 décembre 2000 dans le journal officiel des Communautés européennes. Ce document important, dans lequel l'Union européenne reconnaît les droits, les libertés et les principes fondamentaux, comporte 54 articles consacrés aux personnes au sein de l'UE⁹⁸ et s'inscrit dans une démarche quasi constitutionnelle⁹⁹.

⁹⁵ Directive (CE) 95/46/CE, *supra* note 58.

⁹⁶ Sophie Nerbonne, « Le Groupe de l'article 29 », (2009) 1 *Legicom aux* pp.37-46.

⁹⁷ Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, Journal officiel des communautés européennes, en ligne : <https://www.europarl.europa.eu/charter/pdf/text_fr.pdf> (consulté le 15 août 2022).

⁹⁸ *Ibid.*

⁹⁹ Projet de Charte des droits fondamentaux de l'Union européenne-Texte des explications relatives au texte complet de la Charte, tel que repris au doc. CHARTE 4487/00CONVENT 50, CHARTE 4473/100REV1-ONVENT 49. Bruxelles : Présidium de la Convention sur la Charte des droits fondamentaux, 19.10.2000. 56p.

La Charte des droits fondamentaux de l'Union européenne comporte désormais un article spécifiquement consacré à la « protection des données personnelles », en effet, en son article 8, que « toute personne a droit à la protection des données à caractère personnel la concernant ». Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un fondement légitime prévu par la loi, toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification » et, finalement, « le respect de ces règles est soumis au contrôle d'une autorité indépendante »¹⁰⁰.

Cette dernière considération juridique a pu sembler offrir aux yeux de certains juristes, un soutien constitutionnel au droit à la protection des données personnelles¹⁰¹ et s'insérant du même coup dans la nécessité d'une refonte paramétrée de la Directive 95/46/CE et dans une certaine mesure d'une ratification du « droit à l'oubli numérique » sans l'ombre d'un doute comme un droit réel et fondamental¹⁰². Et finalement consacré au Règlement (UE) 2016/679 et particulièrement à son article 17 déjà visité par notre analyse du sujet¹⁰³.

¹⁰⁰ Charte des droits fondamentaux de l'Union européenne, *supra* note 97.

¹⁰¹ Paul De Hert et Serge Gutwirt, *Data Protection in the Case Law of Strasbourg, and Luxembourg: Constitutionalisation in action*, 2009 aux pp.3-44.

¹⁰² *Digital Rights Ireland Ltd et Michael Seitlinger e.a.*, affaires jointes C-293/12 & C-594/12, CJUE, Grande Chambre, 8 avril 2014. Pour un commentaire éclairant de cette affaire, lire la lettre ADL du 14 mai 2014 de Marie-Laure Basilien-Gainche.

¹⁰³ Règlement (UE) 2016/679, *supra* note 72.

1.11 Les décisions marquantes du droit à l'oubli

L'objectif de cette section est de présenter les décisions marquantes qui, selon notre étude, ont été les plus importantes dans l'évolution du droit à l'oubli. À cet effet, il convient de préciser le critère utilisé pour estimer l'importance d'une décision qui est l'illustration de la problématique du sujet et qui permet de comprendre comment le droit s'est adapté pour offrir une solution à ce problème. À cet égard, il n'est pas étonnant que l'ensemble de ces décisions portent sur la dimension évolutive qui a forgé le droit à l'oubli sur sa perspective informationnelle de la vie privée et sur la protection des données personnelles, en considérant le contexte qu'engendre l'évolution rapide des technologies numériques et l'Internet.

1.12 L'affaire Landru 1965

Comme nous l'avons mentionné dans notre genèse, la première mention dépitée du droit à l'oubli est sous la plume du professeur de droit français Gérard Lyon-Caen¹⁰⁴ dans ses annotations critiques de l'affaire « Landru » de 1965¹⁰⁵, commentant le jugement en 1966.

Dans cette affaire, le juge a alors évoqué une « prescription du silence » établissant un lien indéniable entre le droit à l'oubli et le droit de la prescription¹⁰⁶. Ce lien se manifeste particulièrement dans le cadre de la prescription extinctive de l'action publique et d'informations qui nous sont plus d'actualité qui repose sur le principe que passé un certain temps, il est superfétatoire de rappeler publiquement les actions de la personne concernée¹⁰⁷. Il ne s'agit pas simplement de voir son passé oublié, mais également de pouvoir profiter du présent paisiblement. Comme l'exprime si bien Maryline Boizard

¹⁰⁴ Définition de « informationnelle » par la Cour Suprême du Canada dans l'arrêt : *R c Dymont* (1988) 2RCS 417. Le juge La Forest, aux para 19 et s, distingue trois dimensions de la vie privée : la dimension territoriale, qui touche à la protection de la vie privée dans les différents lieux, la dimension personnelle, qui porte sur la protection du corps et des substances corporelles de la personne et la dimension informationnelle, qui porte sur la protection des renseignements.

¹⁰⁵ Affaire Landru, *supra* note 42.

¹⁰⁶ *Ibid.*

¹⁰⁷ *Ibid.*

(Directrice adjointe de l'Institut de recherche droit et Europe) : « C'est précisément pour éviter les conséquences néfastes ou douloureuses de rappels d'information que le concept de droit à l'oubli a été imaginé »¹⁰⁸.

1.13 L'arrêt M. c. Filipacci 1983

Nous avons également révélé l'importance de l'arrêt de *M c. Filipacchi et Cogédipresse* du 20 avril 1983¹⁰⁹. Dans cette affaire, le tribunal de grande instance de Paris semble s'éloigner de la notion « prescription du silence » considérant qu'elle laissait supposer une certaine automation de l'oubli.

Alors que ce genre d'affaires doit s'apprécier au cas par cas, selon le juge en fonction des intérêts en cause¹¹⁰. La notion de droit à l'oubli va donc être privilégiée par la Cour et s'introduire dans le droit positif par la voie de la responsabilité civile¹¹¹. Dans cette cause, le juge s'efforce de trouver un équilibre entre le droit à l'information et le droit à l'oubli de la personne concernée de nouveaux stigmatisés dans la publication de Cogédipresse. Il consacre ce droit avec la citation suivante : « Attendu que toute personne qui a été mêlée à des événements publiés peut, le temps passant, revendiquer le droit à l'oubli »¹¹². D'autres décisions ont suivi dans lequel était revendiqué le droit à l'oubli sur les mêmes bases juridiques, mais ce contentieux restait relativement marginal et le droit à l'oubli semblait incertain et hypothétique en Europe¹¹³.

Il faudra attendre en 2014 pour la Cour de justice de l'Union européenne (CJUE) qui ouvre le débat sur le droit à l'oubli directement dans l'arrêt Google Spain.

¹⁰⁸ Maryline Boizard, « Le Temps, le droit à l'oubli et le droit à l'effacement », (2016) 4 : 2 Les Cahiers de justice, 620.

¹⁰⁹ M.c. Fillipacchi et Cogedipresse, *supra* note 43.

¹¹⁰ Letteron *supra* note 38

¹¹¹ *Ibid.*

¹¹² *Ibid.*

¹¹³ Boizard, *supra* note 108.

1.14 L'affaire Google Spain

Le 13 mai 2014, la Cour de justice de l'Union européenne (CJUE) est saisie d'une demande de décision préjudicielle introduite par l'Audiencia Nacional espagnole. La demande faisait suite à un litige opposant Google Spain SL et Google Inc. à l'Agence espagnole de protection des données et à M. Costeja Gonzales¹¹⁴. M. Gonzales avait préalablement introduit auprès de l'Agence espagnole de protection des données une réclamation à l'encontre du journal espagnol La Vanguardia, de Google Spain et Google Inc. La demande d'instance portait sur le fait que lorsqu'un utilisateur du moteur de recherche inscrivait le nom complet de M. Gonzales au moteur de recherche de Google, l'internaute obtenait deux articles de 1998 du même journal La Vanguardia dans lequel se trouvait une annonce de la vente aux enchères liée à une saisie de recouvrement des dettes pratiqué sur les biens de M. Gonzalez eu raison de son insolvabilité¹¹⁵. Dans les faits, M. Gonzales entreprend alors plusieurs démarches auprès du journal espagnol et de Google pour que les pages et les liens soient supprimés. Sa demande reste sans réponse. Le litige vient du seul fait du refus de ses deux antagonistes de donner suite à la demande de M. Gonzales. Considérant cette situation, ce dernier n'a d'autre choix que de s'adresser à l'Agence espagnole de protection des données de prendre fait et cause pour lui et d'ordonner aux exploitants du moteur de recherche Google de retirer les pages et liens du journal la Vanguardia¹¹⁶. En expliquant toutefois que ladite saisie dont il avait fait l'objet et rapportée par le journal avait été entièrement réglée depuis de nombreuses années, que la publication et diffusion de celle-ci constitue une entrave à sa vie privée¹¹⁷.

À la suite de cette requête de M. Gonzalez, l'Agence espagnole de la protection des données (AEPD) réitère sa demande contre le journal la Vanguardia en estimant que l'éditeur avait légalement publié les informations en cause. Cependant, l'Agence (AEPD) a cependant accueilli la demande à l'encontre de Google Spain et de Google Inc. Ladite

¹¹⁴ Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD), *supra* note 7.

¹¹⁵ *Ibid* à la p 6.

¹¹⁶ *Ibid*.

¹¹⁷ *Ibid*.

agence a alors demandé à ces deux sociétés de prendre les mesures nécessaires pour retirer les données de leur indexe (désindexer les pages problématiques) pour les rendre d'atteinte impossible¹¹⁸. La réaction de Google Spain et Google Inc. fut d'introduire deux recours séparés contre la décision devant l'Audiencia Nacional (Audience nationale espagnole), ayant comme conclusion l'annulation de la décision de l'Agence espagnole de la protection des données à leur égard. Conséquemment, la Juridiction nationale espagnole a présenté une multitude de questions préjudicielles à la Cour de justice de l'Union européenne¹¹⁹.

1.15 Pour un souci de clarté

Le renvoi préjudiciel devant la Cour de justice de l'Union européenne est une procédure du droit de l'Union européenne par laquelle les juridictions des États membres interrogent la Cour de justice de l'Union européenne sur l'interprétation des traités européens ou sur l'interprétation ou la validité d'un acte du droit dérivé de l'Union européenne. La demande d'interprétation faite devant la Cour est qualifiée de question préjudicielle, et l'exception par laquelle une partie à l'instance conteste l'interprétation ou la validité de l'acte est qualifiée d'exception préjudicielle¹²⁰.

Les questions préjudicielles posées à la Cour de justice de l'Union européenne visaient de savoir si l'activité d'un moteur de recherche peut être considérée de « traitement de données à caractère personnel » ? L'exploitant du moteur de recherche doit-il être qualifié comme « responsable du traitement de ces données ? Le groupe du moteur de recherche installé dans un État membre peut-il être considéré comme étant un « établissement local » de nature à provoquer l'applicabilité du droit national de cet État ? Une autorité nationale

¹¹⁸ *Ibid* à la p 7

¹¹⁹ *Ibid* à la p 1.

¹²⁰ Cette procédure est jugée utile lorsque, dans le cadre d'une affaire devant un juridiction nationale, une nouvelle question d'interprétation d'intérêt général se pose pour l'application uniforme du droit de l'UE, ou lorsque la jurisprudence existante ne semble pas donner d'orientation permettant de traiter une nouvelle situation juridique. Ces recommandations expliquent aux juridictions nationales des pays de l'Union européenne (UE) les objectifs d'une procédure qui les autorise, conformément à l'article 267 du TFUE, à consulter la Cour de justice de l'Union européenne (CJUE) à titre préjudiciel. Cette procédure est utilisée dans les cas où l'interprétation ou la validité du droit de l'UE est remise en cause et : lorsqu'une décision doit permettre à une juridiction nationale de rendre son jugement ; lorsqu'il n'existe aucun recours juridictionnel dans le droit national. Ces recommandations prévoient également le champ d'application de la procédure et la forme sous laquelle les juridictions nationales doivent effectuer la demande de renvoi. Elles viennent compléter les articles 93 à 118 du règlement de procédure de la CJUE. Voir procédures préjudicielles : recommandations à l'attention des juridictions nationales, en ligne : <<https://eur-lex.europa.eu/FR/legal-content/summary/preliminary-ruling-proceedings-recommendations-to-national-courts.html>> (consulté le 15 août 2022).

peut-elle ordonner au moteur de recherche qu'il procède au déréférencement sur les pages d'informations publiées par des tiers sans s'adresser à ces tiers, y compris lorsque les informations ont été légalement publiées ? Une personne physique bénéficie-t-elle du droit à la suppression des liens dans les pages de résultats de recherche, même s'il s'agit des informations qui ont été publiées légalement ?¹²¹

Et plus particulièrement, à connaître quelles obligations incombent aux exploitants de moteur de recherche sur le plan de protection des données à caractère personnel, lorsque les personnes concernées ne souhaitent pas que ces données soient mises à la disposition des utilisateurs d'Internet de façon indéterminée¹²². La réponse résultait de l'interprétation de la Directive 95/46/CE¹²³ en considérant l'évolution des technologies et l'Internet des dernières années. Comme nous l'avons déjà vu, cette directive du 24 octobre 1995 est relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et a pour objectifs, conformément à son article 1, paragraphe 1, d'assurer la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel¹²⁴. La Cour devait au préalable déterminer si la Directive 95/46/CE est applicable en l'espèce. Ce qui par ailleurs n'était pas acquis, puisque cela obligeait, pour la CJUE, d'établir la responsabilité d'un exploitant d'un moteur de recherche ayant son siège social dans un pays non-membre de l'Union européenne.

La Cour de justice de l'Union européenne, en plus de reconnaître les droits des personnes concernées par le traitement de données personnelles et établir la responsabilité de l'exploitant de moteurs de recherche, la Cour a dû interpréter de manière adaptative la Directive 95/46/CE pour correspondre à la réalité contemporaine du litige¹²⁵. Malgré les

¹²¹ Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD), *supra* note 7

¹²² *Ibid.*

¹²³ Décision-cadre 2008/977/JI, *supra* note 65.

¹²⁴ La directive CE 95/46, *supra* note 58 à l'article 1, paragraphe 1.

¹²⁵ V.L. Benabou et J. Rochfeld, « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? » (2014) 25 Recueil Dalloz, 1476.

difficultés d'interprétation de la directive, la CJUE a reconnu, dans un premier temps, son applicabilité et, d'autre part, estime que : « l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichés à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages Web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom et où ces informations ne sont pas effacées préalablement ou simultanément de ces pages Web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite »¹²⁶.

Même un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Tel est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard de ces finalités et du temps qui s'est écoulé¹²⁷.

Poursuivons le raisonnement de la CJUE, comme déjà précisé, pour répondre aux questions en litige qui lui étaient posées, la Cour de justice de l'Union européenne devait répondre auparavant à l'applicabilité de la Directive 95/46/CU, si un exploitant du moteur de recherche procède à une collecte des « données générales », ce qui inclut des données à caractère personnel d'une manière automatisée et systématique, constitue une collecte de données au sens de ladite directive. Pour répondre à cette question, la Cour rappelle la définition de « données à caractère personnel » de la façon suivante :

À cet égard, il y a lieu de relever que l'article 2, sous b), de la Directive 95/46 définit le « traitement de données à caractère personnel » comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction¹²⁸.

¹²⁶ Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD), *supra* note 7 au para 88.

¹²⁷ *Ibid* au para 93.

¹²⁸ *Ibid* au para 25.

Or, selon la CJUE, chacune des activités de l'exploitant d'un moteur de recherche implique la collecte, l'extraction, l'enregistrement, l'organisation, la conservation et la communication ou mise à disposition des données personnelles sous la forme de résultat d'une recherche sur Internet doit être qualifiée de « traitement » de données à caractère personnel. Et ce, indépendamment du fait que l'exploitant du moteur de recherche les applique sans les différencier des informations générales¹²⁹.

Il ne faisait donc pas de doute pour la Cour que parmi les résultats de recherche mis à disposition des utilisateurs des informations figuraient sur des personnes physiques identifiées ou identifiables. « En ce qui concerne l'activité en cause au principal, il n'est pas contesté que parmi les données trouvées, indexées, stockées par les moteurs de recherche et mises à la disposition de leurs utilisateurs figurent également des informations concernant des personnes physiques identifiées ou identifiables et donc des « données à caractère personnel » au sens de l'article 2, sous a), de cette directive »¹³⁰.

La Cour précise également dans cette affaire, que les opérations visées par la Directive 95/46UE doivent être qualifiées de « traitement » même si ces les données ont déjà fait l'objet d'une publication sur Internet et ne sont pas modifiés par ce moteur de recherche¹³¹. On remarque à travers l'argumentation de la CJUE, sa volonté d'adapter les effets à la directive 95/4/CE, afin de pouvoir réguler les activités des opérateurs de moteurs de recherche¹³².

La question relative de la notion « responsable du traitement » de données personnelles est adressée par la Cour de la manière suivante :

Il convient de rappeler que l'article 2, sous d) de la Directive 95/46 définit celui-ci comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul

¹²⁹ *Ibid* au para 28.

¹³⁰ *Ibid* au para 27.

¹³¹ *Ibid* au para 29.

¹³² *Ibid* au para 30.

ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel¹³³.

Cela étant, pour que la directive s'applique en cette circonstance, la CJUE a dû passer par la norme européenne, tel que défini sous la directive, pour conclure que « c'est l'exploitant du moteur de recherche qui détermine les finalités et les moyens de cette activité et ainsi du traitement de données à caractère personnel qu'il effectue, lui-même, dans le cadre de celle-ci et qui doit, par conséquent, être considéré comme le « responsable de ce traitement »¹³⁴.

Il convient également de souligner que pour l'exploitant du moteur de recherche lequel incombe le traitement de données personnelles considérant son rôle et son activité se distinguerait de celui de l'éditeur de sites Web, mais elle s'y ajouterait selon l'interprétation de la Cour. Sur ce, la Cour s'exprime ainsi :

À cet égard, il y a lieu de souligner que le traitement de données à caractère personnel effectué dans le cadre de l'activité d'un moteur de recherche se distingue et s'ajoute à celui effectué par les éditeurs de site Web, consistant à faire figurer ces données sur une page Internet¹³⁵.

La Cour convient qu'il serait contraire au libellé clair et à l'objectif de la définition large de la notion de « responsable », d'exclure de celle-ci l'exploitant d'un moteur de recherche pour les raisons qu'il n'exerce pas un contrôle sur les informations à caractère personnel publiées sur la page Internet de tiers¹³⁶.

La qualité de responsable du traitement de données à caractère personnel qui incombe aux exploitants de recherche est également due selon la CJUE au fait « qu'il est constant que cette activité des moteurs de recherche joue un rôle décisif dans la diffusion globale desdites données en ce qu'elle rend celles-ci accessibles à tout internaute effectuant une

¹³³ *Ibid* au para 32.

¹³⁴ *Ibid au* para 33.

¹³⁵ *Ibid au* para 35.

¹³⁶ *Ibid au* para 34.

recherche à partir du nom de la personne concernée, y compris aux internautes qui, autrement, n'auraient pas trouvé la page Web sur laquelle ces mêmes données sont publiées »¹³⁷.

La facilité à diffuser l'information des moteurs de recherche sous la gouverne de l'exploitant devient pour la Cour un considérant de responsabilité. De plus, l'organisation et l'agrégation des informations publiées sur Internet effectuées par les moteurs de recherche dans le but de faciliter à leurs utilisateurs l'accès à celles-ci peuvent conduire, lorsque la recherche de ces derniers est effectuée à partir du nom d'une personne physique, à ce que ceux-ci obtiennent par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvable sur Internet leur permettant d'établir un profil plus ou moins détaillé de la personne concernée¹³⁸.

En considération du fait que l'exploitant du moteur de recherche détermine la finalité et les moyens du traitement des données au sein de la recherche, ces derniers assument donc la responsabilité du traitement que son activité a produit envers les personnes concernées et des effets éventuels sur leur vie privée. C'est ce qui apparaît au paragraphe 38 de la décision.

Dans la mesure où l'activité d'un moteur de recherche est donc susceptible d'affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites Web les droits fondamentaux de la vie privée et de la protection de données à caractère personnel, l'exploitant de ce moteur en tant que personne déterminant les finalités et les moyens de cette activité doit assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que celle-ci satisfait aux exigences de la Directive 95/46 pour que les garanties prévues par celle-ci puissent développer leur plein effet et qu'une

¹³⁷ *Ibid* au para 36.

¹³⁸ *Ibid* au para 37.

protection efficace et complète des personnes concernées, notamment de leur droit au respect de leur vie privée, puisse effectivement être réalisée¹³⁹.

En interprétant d'une façon généreuse la notion de « responsable des données », ce qui répondait à la réalité actuelle de l'avancement des technologies et particulièrement l'Internet, la Cour de justice de l'Union européenne estime qu'il a lieu d'inclure de cette responsabilité l'exploitant d'un moteur de recherche. C'est sans équivoque que la Cour se prononce et fait valoir sa position de la façon suivante :

Il découle de l'ensemble des considérations qui précèdent qu'il convient de répondre à la deuxième question, sous a) et b), que l'article 2, sous b) et d), de la Directive 95/46 doit être interprété en ce sens que, d'une part, l'activité d'un moteur de recherche consistant à trouver de informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et enfin, à les mettre à la disposition des internautes selon un ordre de préférence donnée doit être qualifiée de « traitement de données à caractère personnel », au sens de cet article 2, sous b), lorsque ces informations contiennent des données à caractère personnel et, d'autre part, l'exploitant de ce moteur de recherche doit être considéré comme le « responsable » dudit traitement, au sens dudit article 2, sous d)¹⁴⁰.

La question importante que la Cour devait résoudre est le champ d'application du droit national de l'Union européenne, en particulier l'applicabilité de la Directive 95/46 UE à l'exploitant de moteur de recherche, alors que le siège social de la société est établi à l'extérieur de l'Union européenne¹⁴¹. Pour déterminer si le responsable du traitement de données à caractère personnel par un exploitant étranger du territoire de l'Union européenne était contraignable, la Cour devait se pencher sur la notion « d'établissement » au sens de l'article 4 du paragraphe 1, sous a), de la Directive 95/46/UE et sur celle de « recours à des moyens situés sur le territoire dudit État membre », au sens du même article, sous c)¹⁴².

¹³⁹ *Ibid* au para 38.

¹⁴⁰ *Ibid* au para 41.

¹⁴¹ *Ibid* au para 42.

¹⁴² *Ibid* au para 44.

En considérant de ce qui précède pour l'application juridictionnelle, la CJUE convient que pour la Directive 95/46 UE peut être appliquée concrètement, il fallait qu'au moins une des trois conditions suivantes soit réunie :

- l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre, ou
- la société mère désigne une filiale implantée dans ledit État membre comme son représentant et comme étant responsable du traitement de deux fichiers spécifiques contenant les données des clients ayant conclu des services publicitaires avec cette entreprise, ou
- la succursale ou la filiale établie dans un État membre transmet à la société mère, basée en dehors de l'Union, les réclamations et les injonctions que lui adressent aussi bien les intéressés que les autorités compétentes une vue d'obtenir le respect du droit à la protection des données à caractère personnel, même lorsque cette collaboration a lieu de manière volontaire¹⁴³.

La Cour en vient donc à statuer que lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à des activités de promotions et de ventes publicitaires offertes par ce moteur de recherche et dont l'activité vise les citoyens du territoire d'un État membre¹⁴⁴, un traitement de données à caractère personnel est effectué « sur le territoire d'un État membre » au sens de la directive¹⁴⁵.

La CJUE a considéré en l'espèce que la première condition était remplie et conclu que :

Un traitement de données à caractère personnel est effectué dans le cadre d'un établissement du responsable de ce traitement sur le territoire d'un État membre [...] lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à

¹⁴³ *Ibid* au para 45.

¹⁴⁴ *Ibid* au para 49.

¹⁴⁵ *Ibid* au para 59.

assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre¹⁴⁶.

Afin de bien comprendre la portée de ce jugement novateur de la Cour de justice de l'Union européenne, il est important de se rappeler que cette dernière cherchait à répondre à des questions d'actualité de 2014 avec des notions législatives de 1995 en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces mêmes données¹⁴⁷. En cette circonstance, la Cour, en premier lieu, estime que Google Spain est une filiale de Google Inc. en Espagne. Dans un second temps, elle a considéré que Google Inc. est le responsable du traitement à caractère personnel par la nature même de ses activités d'un établissement (filiale) appartenant à ce même responsable qui selon les faits est situé dans un État membre de l'Union européenne. Dans ce contexte, la Cour pose les assises de son jugement et précise au paragraphe 53 qu'au « vue de l'objectif de la Directive 95/46 d'assurer une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privée à l'égard du traitement des données à caractère personnel, cette dernière expression » ne saurait recevoir une interprétation restrictive¹⁴⁸. La Cour explique également au considérant du paragraphe 55 de la notion des « activités » de l'établissement que :

Compte tenu de cet objectif de la Directive 95/46 et du libellé de son article 4, paragraphe 1, sous a), il y a lieu de considérer que le traitement de données à caractère personnel qui est fait pour les besoins du service d'un moteur de recherche tel que Google Search, lequel est exploité par une entreprise ayant son siège dans un État tiers, mais disposant d'un établissement dans un État membre, est effectué « dans le cadre des activités » de cet établissement si celui-ci est destiné à assurer, dans cet État membre, la promotion et la vente des espaces publicitaires proposés par ce moteur de recherche, qui servent à rentabiliser le service offert par ce moteur¹⁴⁹.

¹⁴⁶ *Ibid* au para 60.

¹⁴⁷ La directive CE 95/46, *supra* note 58.

¹⁴⁸ Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD), *supra* note 7 au para 53.

¹⁴⁹ *Ibid* au para 55.

La CJUE relève que

les activités de l'exploitant du moteur de recherche et celles de son établissement situé dans l'État membre concerné sont indissociablement liées. Dès lors que les activités relatives aux espaces publicitaires constituent le moyen pour rendre le moteur de recherche en cause économiquement rentable et que ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activités¹⁵⁰.

La Cour rappelle à son paragraphe 57 et éclaircit la notion de « traitement » de données en ces mots :

L'affichage même de données à caractère personnel sur une page de résultats d'une recherche constitue un traitement de telles données. Or, ledit affichage de résultats étant accompagné, sur la même page, de celui de publicités liées aux termes de recherche, force est de constater que le traitement de données à caractère personnel en question est effectué dans le cadre de l'activité publicitaire et commerciale de l'établissement du responsable du traitement sur le territoire d'un État membre, en l'occurrence le territoire espagnol¹⁵¹.

Or, la Cour retient et considère que l'activité commerciale à la base du modèle économique des opérateurs de services Internet doit être prise en compte considérant que son établissement joue un rôle important dans le traitement de données à caractère personnel, s'il est fusionné à une publicité ciblée aux citoyens de l'État en cause. Elle conclut donc que ledit moteur de recherche ne peut se soustraire « aux obligations et aux garanties prévues par la Directive 95/46/UE, ce qui porterait atteinte à l'effet utile de celle-ci et à la protection efficace et complète des libertés et de droits fondamentaux des personnes »¹⁵².

Il ressort de ce qui précède que Google est soumis aux droits de l'Union européenne, bien que le moteur de recherche soit exploité par une entreprise étrangère à l'Union européenne, sa filiale espagnole qui a comme activités commerciales le traitement de données à

¹⁵⁰ *Ibid* au para 56.

¹⁵¹ *Ibid* au para 57.

¹⁵² *Ibid* au para 58.

caractère personnel afin de cibler la société espagnole pour vendre de la publicité au bénéfice de la maison-mère, soit Google Inc.

Bien que la Cour de justice de l'Union européenne conclut à l'application de la Directive 95/46/UE à l'affaire dont elle était saisie, la Cour devait décider quelles obligations l'exploitant du moteur de recherche Google qui était désormais reconnu comme responsable du traitement de données à caractère personnel lui était soumis et de quelle manière. Autrement dit, quels sont les effets de ladite directive sur Google.

Pour ce faire, la Cour fait premièrement référence selon lesquels les droits fondamentaux font partie intégrante des principes essentiels du droit parmi duquel elle doit assurer le respect et qui sont dorénavant inscrits dans la Charte des droits fondamentaux de l'Union européenne¹⁵³. Cela laissant déjà présager la confrontation parmi les différents droits ainsi protégés à la Charte de l'Union européenne.

La Cour devrait décidément harmoniser les droits divergents de la présente affaire, particulièrement, le droit à la vie privée, incluant le droit à la protection des données personnelles et la liberté d'expression et d'information. La Cour devait donc trancher entre un droit d'intérêt privé et un droit à caractère public.

La CJUE a conclu, aux termes de ce procès à la prédominance au respect de la vie privée et à la protection des données à caractère personnel, elle nous rappelle que « La Cour a déjà jugé que les dispositions de la Directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptible de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux qui, selon une jurisprudence constante, font partie intégrante des principes généraux du droit dont la Cour assure le respect et qui sont désormais inscrits dans la Charte »¹⁵⁴ et que l'article 8 de la Charte dispose de la manière de traiter les données

¹⁵³ Union européenne, Conseil, Parlement et Commission de l'Union européenne, 50^{ème} année (2007/C 303/01), Charte des droits fondamentaux de l'Union européenne, JOUE C.303/1, 14 décembre 2007

¹⁵⁴ Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD), *supra* note 7 au para 68.

personnelles spécifiquement. Ainsi, l'article 7 de la Charte garantit le droit au respect de la vie privée, tandis que l'article 8 de la Charte proclame expressément le droit à la protection des données à caractère personnel. Les paragraphes 2 et 3 de ce dernier article précisent que ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi, que toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification et que le respect de ces règles est soumis au contrôle d'une autorité indépendante. Ces exigences sont mises en œuvre notamment par les articles 6,7-12,14 et 28 de la Directive 95/46¹⁵⁵.

La Cour explique à son paragraphe 70 en outre, l'article 12 sous, b), de la Directive 95/46 UE, conçoit et dispose que les États membres « garantissent à toute personne concernée le droit d'obtenir du responsable du traitement, selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la Directive 95/46, notamment en raison du caractère incomplet ou inexact des données. Cette dernière précision relative au cas du non-respect de certaines exigences visées à l'article 6, paragraphe 1, sous d) de la Directive 95/46 révélant un caractère exemplatif et non exhaustif, il s'ensuit que la non-conformité du traitement, susceptible d'ouvrir à la personne concernée le droit garanti à l'article 12, sous b), de ladite directive, peut également découler du non-respect des autres conditions de licéité imposées par celle-ci au traitement de données à caractère personnel »¹⁵⁶.

À cet égard, la CJUE précise sans équivoque l'étendue du droit à la protection des données à caractère personnel et les obligations contraignantes pour les exploitants de moteurs de recherche.

En considération de ce précède, la Cour conclut et a appliqué les mesures législatives prévues de la directive au traitement numérique des données par les exploitants de moteurs de recherche, elle dispose qu'« il incombe au responsable du traitement d'assurer que les

¹⁵⁵ *Ibid* au para 69.

¹⁵⁶ *Ibid* au para 70.

données à caractère personnel sont « traitées loyalement et licitement », qu'elles sont « collectées pour des finalités déterminées, explicites et légitimes, et [ne sont pas] traitées ultérieurement de manière incompatible avec ces finalités », qu'elles sont « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement », qu'elles sont « exactes et, si nécessaire, mises à jour » et, enfin, qu'elles sont « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Dans ce contexte, ce responsable doit prendre toutes les mesures raisonnables pour que les données qui ne répondent pas aux exigences de cette disposition soient effacées ou rectifiées »¹⁵⁷.

Concrètement, l'obligation à la charge du « responsable » à savoir, l'exploitant du moteur de recherche « doit prendre toutes les mesures raisonnables » pour que les données à caractère personnel qui ne répondent plus ou pas aux exigences des dispositions de la Directive 95/46/UE soient effacées ou rectifiées.

La CJUE explique la procédure à suivre pour la personne concernée dont les données personnelles subissent un traitement, cette dernière peut demander au responsable de mettre fin au traitement desdites données et exiger leur retrait. Si le responsable du traitement ne donne pas suite, la personne concernée peut saisir l'autorité de contrôle ou judiciaire¹⁵⁸.

En effet, une personne peut s'adresser préalablement ou en même temps au propriétaire du site Internet sur lequel se présentent les informations la concernant et à l'exploitant d'un moteur de recherche sans distinction au principe de subsidiarité. La Cour affirme que l'exploitant du moteur de recherche a l'obligation à certaines conditions énumérées à la directive 95/45/UE de supprimer les résultats obtenus à la suite d'une recherche effectuée à partir du nom d'une personne. Pour plus de clarté, l'exploitant doit supprimer de la liste

¹⁵⁷ *Ibid* au para 72.

¹⁵⁸ *Ibid* au para 77.

des résultats, les liens vers les pages Internet, même si parfois la publication par les tiers pourrait subsister indépendamment de la licéité des données¹⁵⁹.

En partant du constat que les droits fondamentaux d'une personne à prééminence non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais aussi sur l'intérêt du public en général à accéder à l'information en question lors d'une recherche ciblée sur le nom de cette personne. Sur ces points, la Cour indique :

Il importe d'emblée de relever que, ainsi qu'il a été constaté aux points 36 à 38 du présent arrêt, un traitement de données à caractère personnel, tel que celui en cause au principal, réalisé par l'exploitant d'un moteur de recherche, est susceptible d'affecter significativement les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel lorsque la recherche à l'aide de ce moteur est effectué à partir du nom d'une personne physique, dès lors que ledit traitement permet à tout internaute d'obtenir par la liste de résultats un aperçu structuré d'informations relatives à cette personne trouvable sur Internet, qui touchent potentiellement à une multitude d'aspects de sa vie privée et qui, sans ledit moteur de recherche, n'auraient pas ou seulement que très difficilement pu être interconnectées, et ainsi d'établir un profil plus ou moins détaillé de celle-ci. En outre, l'effet de l'ingérence dans lesdits droits de la personne concernée se trouve démultiplié en raison du rôle important que jouent Internet et les moteurs de recherche dans la société moderne, lesquels confèrent aux informations contenues dans une telle liste de résultats un caractère ubiquitaire¹⁶⁰.

Et elle précise que :

Au vu de la gravité potentielle de cette ingérence, force est de constater que celle-ci ne saurait être justifiée par le seul intérêt économique de l'exploitant d'un tel moteur dans ce traitement. Cependant, dans la mesure où la suppression de liens de la liste de résultats pourrait, en fonction de l'information en cause, avoir des répercussions sur l'intérêt légitime des internautes potentiellement intéressés à avoir accès à celle-ci, il y a lieu de rechercher, dans des situations telles que celles en cause au principal, un juste équilibre notamment entre cet intérêt et les droits fondamentaux de cette personne au titre des articles 7 et 8 de la Charte. Si, certes, les droits de la personne concernée protégés par ces articles prévalent également, en règle générale, sur ledit intérêt des internautes, cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier notamment, en fonction du rôle joué par cette personne dans la vie publique¹⁶¹.

¹⁵⁹ *Ibid* au para 82.

¹⁶⁰ *Ibid* au para 80.

¹⁶¹ *Ibid* au para 81.

En conclusion, la CJUE estime donc, « l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, les liens des pages Web, publiées par des tiers et contenant des informations relatives à cette personne »¹⁶².

1.16 Reconnaissance du droit à l'oubli par la CJUE

La Cour reconnaît nommément l'existence du droit à l'oubli, non seulement, par l'effet de déduction du dispositif de l'arrêt, mais de manière nominative. Elle concrétise que la Directive 95/46/UE devra dorénavant être interprétée de façon qu'ils « permettent à la personne concernée d'exiger de l'exploitant d'un moteur de recherche de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom de cette personne, des liens vers des pages Web, publiées légalement par des tiers et contenant des informations véridiques relatives à cette dernière, au motif que ces informations sont susceptibles de lui porter préjudice ou qu'elle désire que celles-ci soient « oubliées » après un certain temps »¹⁶³.

En cette cause, la Cour rappelle au paragraphe 91 :

M. Costeja Gonzalez ainsi que les gouvernements espagnol et italien sont de l'avis que la personne concernée peut s'opposer à l'indexation de ses données personnelles par un moteur de recherche lorsque la diffusion de ces données par l'intermédiaire de celui-ci lui porte préjudice et que ses droits fondamentaux à la protection desdites données et au respect de la vie privée, lesquels englobent le « droit à l'oubli », prévalent sur les intérêts légitimes de l'exploitant dudit moteur et l'intérêt général à la liberté d'information¹⁶⁴.

Ce paragraphe tel que rapporté par la CJUE de façon intentionnelle nous laisse penser que la Cour reconnaît expressément le droit à l'oubli comme faisant partie intégrante du respect de la vie privée, et d'ailleurs cette dernière répond par l'affirmative à M. Gonzalez et il est

¹⁶² *Ibid* au para 88.

¹⁶³ *Ibid* au para 89.

¹⁶⁴ *Ibid* au para 91.

dans ses droits de se faire « oublier » lorsque la diffusion de ces données par l'intermédiaire de l'exploitant dudit moteur de recherche lui porte préjudice. La Cour dispose :

Il découle de ces exigences, prévues à l'article 6, paragraphe 1, sous c) à e), de la Directive 95/46, que même un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Tel est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard de ces finalités et du temps qui s'est écoulé¹⁶⁵.

Nonobstant, la reconnaissance de la Cour de ce droit, l'existence du droit à l'oubli est conditionnelle à l'existence d'un débiteur identifié, à savoir le responsable du traitement des données et « le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à savoir, du fait de cette inclusion, accès à l'information en question »¹⁶⁶.

Néanmoins, l'ensemble des considérations établies par la Cour qui précède démontre la primauté incontestable du droit à l'effacement des données à caractère personnel, « non seulement sur l'intérêt économique de l'exploitant du moteur de recherche », mais également sur l'intérêt des internautes¹⁶⁷.

La Cour de justice de l'Union européenne par cette décision du 13 mai 2014 réussit un exercice de force en conciliant une directive de 1995 à la réalité de l'Internet de 2014 et confère à sa propre décision une portée extraterritoriale en faisant du cyberspace une sphère de droit applicable.

Pour l'instigateur de cette importante affaire, M. Mario Costeja Gonzalez dans son intention de se faire oublier son passé, c'est peine perdue puisque quelques mois plus tard

¹⁶⁵ *Ibid* au para 93.

¹⁶⁶ *Ibid* aux para 97-99.

¹⁶⁷ *Ibid* au para 97.

après la publication de ce jugement les requêtes effectuées avec son nom dépassaient les quarante mille (40 000) résultats¹⁶⁸.

Cette cause fut fondamentale pour jeter les fondations du droit à l'oubli numérique et son apport au corpus jurisprudentiel européen.

1.17 La cause emblématique d'une chirurgienne néerlandaise

Le tribunal d'Amsterdam a rendu une importante décision sur le droit à l'oubli en date du 19 juillet 2018 qui opposait Google LLC (anciennement Google Inc.) et une chirurgienne néerlandaise¹⁶⁹.

En préambule, nous vous faisons remarquer que le nom des demandeurs ou personnes concernées dans leur requête d'attribution de suppression de données personnelles des résultats de recherche à l'exploitant du moteur de recherche n'apparaît plus sur les actes de procédures juridiques. Effectivement, depuis la décision Google Spain de 2014, les demandeurs sont autorisés par la nature de la procédure de taire leur nom, cela semble s'imposer spontanément à l'esprit puisque le but est de se « faire oublier » alors que les procédures judiciaires emportent souvent une notoriété plus accrue du nom de la personne associée aux dites procédures¹⁷⁰.

Les faits de l'affaire sont les suivants : une chirurgienne qui avait été sanctionnée par le tribunal disciplinaire régional des soins de santé à une suspension sans condition de son inscription au registre en ligne néerlandaise pour les professionnels de la santé (il est

¹⁶⁸ Stéphanie Dalet-Venot, « Affaire Google Spain : L'affirmation d'un droit à l'oubli », Legavoix.fr (10 septembre 2014) en ligne (blogue) : <<https://www.legavox.fr/blog/e-reputation-et-droit/affaire-google-spain-affirmation-droit-16075.htm>>

¹⁶⁹ Tribunal de district d'Amsterdam, C/13/636885/HA_KK_17-30/, jugement du 19 juillet 2018 publication 18 décembre 2018, en ligne : <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2018:8606>

¹⁷⁰ Dalet-Venot, *supra* note 168. Dans les faits Monsieur Gonzalez a agi à titre de demandeur dans l'arrêt Google Spain. À la suite de la publication dudit arrêt, les requêtes effectuées à partir de son nom sur Google aboutissent à des milliers de résultats, le rendant célèbre malgré lui. Ce qu'il voulait à tout prix éviter.

obligatoire pour un médecin d'être inscrit au registre pour pouvoir exercer leur profession ou utiliser leur titre professionnel)¹⁷¹.

Après un appel, le Tribunal disciplinaire central des soins de santé a annulé la décision antérieure pour la remplacer par une suspension conditionnelle en vertu de laquelle la requérante a été autorisée à continuer d'exercer avec une période probatoire, ce qui dans la présente cause devait avoir comme effet sa réinscription au registre en ligne¹⁷². Le litige envers la chirurgienne s'invite de cette manière : les premiers résultats d'une recherche avec le nom de cette dernière au moteur de recherche Google référaient toujours via un lien vers un site Internet contenant une liste de praticiens, de médecins et d'autres professionnels de la santé blâmables et incompetents dans un répertoire « noir » non officiel¹⁷³. La page source de ce lien contenait les informations non remplacées par l'appel de la demanderesse, mais aussi des photos¹⁷⁴. Il ressort des faits de cette affaire que des patients potentiels ayant trouvé la liste « noire » sur Google discutaient ensemble du cas de la demanderesse via un forum Internet. Google et l'organisme néerlandais de surveillance de la confidentialité de données ont initialement rejeté les demandes de suppression des liens en raison que la chirurgienne était toujours en probation et que les informations restaient pertinentes pour le public¹⁷⁵.

En conséquence, la demande vise à ordonner à Google de supprimer les résultats de recherche sur les liens nuisibles et injustes pour la personne concernée, ainsi que d'autres liens reliés aux pages sources ou repris sur le même sujet¹⁷⁶.

Dans cette affaire, il juge que la chirurgienne avait un intérêt légitime à ce que son nom ne soit pas instantanément associé à une liste « noire de médecins » à chaque fois qu'un

¹⁷¹ Tribunal de district d'Amsterdam, *supra* note 169 aux para 2 à 5.

¹⁷² *Ibid* au para 2.7.

¹⁷³ *Ibid*.

¹⁷⁴ *Ibid* au para 2.8.

¹⁷⁵ *Ibid* aux para 2.10,2.2, 2.12.

¹⁷⁶ *Ibid* au para 3.1.

internaute en fait la requête sur Internet et que cet intérêt était « supérieur à l'intérêt du public de pouvoir découvrir cette information de cette manière » et incomplète¹⁷⁷.

La Cour indique que la demande doit être appréciée sur la base subsidiaire de l'article 17 du RGPD, en tenant compte des principes énoncés¹⁷⁸ que nous citons :

Le traitement des données tel que le présent est basé sur l'article 6, point f) du RGPD, qui – dans la mesure pertinente ici – prescrit que le traitement des données à caractère personnel n'est licite que si le traitement ou d'un tiers, sauf si les intérêts ou les libertés et droits fondamentaux de la personne concernée qui nécessitent la protection des données à caractère personnel l'emportent sur ces intérêts¹⁷⁹.

En se référant à l'arrêt Costeja de la CJUE mentionné aux points 3.3 et 4.2 ci-dessus, que les droits fondamentaux d'une personne physique tels que visés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (la Charte) (le Droit au respect de la vie privée et le Droit à la protection des données à caractère personnel) l'emportent généralement sur l'intérêt économique de l'exploitant du moteur de recherche et de l'intérêt légitime des internautes susceptibles d'accéder aux résultats de recherche respectifs. Cela peut être différent dans des cas particuliers, en fonction de la nature de l'information concernée et de sa sensibilité à la vie privée de la personne concernée et de l'intérêt public à disposer de cette information, déterminée notamment par le rôle que cette personne joue dans la vie publique. Dans ce contexte, l'exploitant du moteur de recherche peut être tenu, sur demande, de s'assurer que certains résultats n'apparaissent pas dans une liste de résultats de recherche, notamment s'ils sont factuellement erronés ou, compte tenu des circonstances de l'espèce, aux fins du traitement sont incomplets ou non pertinents ou excessifs au regard des finalités du traitement, parce qu'ils ont des finalités du traitement, parce qu'ils n'ont pas été mis à jour, ou parce qu'ils sont conservés plus longtemps que nécessaire, ou s'il existe des raisons impérieuses et justifiées, relatives à la situation personnelle du demandeur de s'opposer à ce que les données le concernant fassent l'objet d'un traitement. Cette obligation peut également exister si les publications elles-mêmes sont citées¹⁸⁰.

Dans la mise en balance des intérêts sur la base de l'article 6, point f), du RGPD, deux droits fondamentaux sont donc en jeu, à savoir, d'une part, le droit à la vie privée et au respect des données à caractère personnel de [la requérante] (articles 7 et 8 de la Charte) et, d'autre part, le droit à la liberté d'informations (article 11 de la Charte) non seulement de Google, mais aussi de (tous) les internautes, les webmasters et les auteurs/fournisseurs d'informations sur Internet. Ce faisant, l'intérêt de [la requérante] à ce que les liens ne puissent plus être trouvés lorsqu'une recherche est effectuée sur son nom doit être comparée à l'intérêt de Google à produire un résultat de recherche fiable via son moteur de recherche et à l'intérêt du public d'obtenir des informations pertinentes via le moteur de recherche¹⁸¹.

¹⁷⁷ *Ibid* au para 4.16.

¹⁷⁸ *Ibid* au para 4.6.

¹⁷⁹ *Ibid* au para 4.7.

¹⁸⁰ *Ibid* au para 4.8.

¹⁸¹ *Ibid* au para 4.9.

Le tribunal a en outre rejeté l'affirmation de Google qui plaidait, selon laquelle sans son moteur de recherche, la plupart des internautes auraient du mal à trouver les informations pertinentes sur le registre de la Commission médicale néerlandaise et que ces dossiers sont déjà publics¹⁸².

Malgré, le caractère public impliquant une négligence médicale de la part de la demanderesse, la Cour conclut comme suit :

Tout bien considéré, force est de conclure qu'en l'espèce il n'y a pas de circonstances particulières qui signifient que le droit de [la requérante] au respect de sa vie privée et de ses données à caractère personnel doit céder le pas à l'intérêt du public. Le traitement des données à caractère personnel de [requérant] via les liens est, de l'avis du tribunal, non pertinent et excessif¹⁸³.

En conséquence, le tribunal d'Amsterdam fait droit à la réclamation et condamne Google à supprimer le lien dans les sept jours du jugement¹⁸⁴.

Cet Arrêt fut confirmé par la Cour d'appel d'Amsterdam le 7 avril 2020, sous l'affichage de demande de suppression des résultats de recherche et sur l'article 17 du Règlement général sur la protection des données (RGPD) « droit à l'oubli »¹⁸⁵.

1.18 Deux arrêts importants du 24 septembre 2019 de la CJUE

Le 24 septembre 2019, la Cour de justice européenne apporte d'importantes précisions sur la mise en œuvre concrète du droit à l'oubli. Comme nous l'avons vu dans l'affaire Google Spain, la base de la décision avait comme assure législative la Directive 95/46/CE de 1995, relative à la protection des personnes physiques à l'égard du traitement des données à

¹⁸² *Ibid* au para 4.16.

¹⁸³ *Ibid*.

¹⁸⁴ *Ibid* au para 4.17.

¹⁸⁵ Cour d'Appel d'Amsterdam, 200.248.187/01, jugement du 7 avril 2020 publication 6 juillet 2020, en ligne : <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHAMS:2020:1270>.

caractère personnel et à la libre circulation de ces données¹⁸⁶. Directive, depuis abrogée et remplacée par le Règlement 2016/679/UE de 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, entrée en vigueur le 25 mai 2018¹⁸⁷. Dans cette cause Google Spain, la Cour avait reconnu « pour les données à caractère personnel, l'obligation de rectifier en cas de traitement illicite et un droit à l'effacement ou droit à l'oubli en cas de traitement légal. La solution développée par le CJUE implique alors une implantation délicate de balancement des intérêts entre le droit à l'information publique et la protection des données personnelles dans le cadre du droit à la vie privée. Un juste équilibre se devait d'être selon « la nature de l'information en question et sa sensibilité pour la vie privée de la personne concernée ainsi que l'intérêt du public à disposer de cette information »¹⁸⁸.

Une fois, le principe du droit à l'oubli reconnu et le déréférencement ordonné, qu'elles sont les balises et la mise en œuvre de ce droit ?

1.19 Mise en œuvre du droit à l'oubli en Europe

C'est justement pour répondre aux importantes questions d'ordre pratique que la Cour de justice de l'Union européenne a rendu le 24 septembre 2019 deux décisions qui répondent chacune d'elles à des questions préjudicielles présentées par le Conseil d'État français. L'un des arrêts porte sur les conditions de déréférencement de liens qui mènent vers des sites contenant de données personnelles à caractère sensible¹⁸⁹. Le deuxième concerne la portée territoriale du droit à l'oubli en vertu du Règlement général sur la protection des données (RPGD)¹⁹⁰.

¹⁸⁶ La directive CE 95/46, *supra* note 65,95/46/CE.

¹⁸⁷ Règlement (UE) 2016/679, *supra* note 72.

¹⁸⁸ Google Spain SL Google Inc. c. Agencia española de protección de Datos (AEPD), *supra* note 7.

¹⁸⁹ CJUE, 24 septembre 2019 aff.C_136/17.

¹⁹⁰ Google LLC, venant aux droits de Google Inc. contre Commission nationale de l'informatique et des libertés (CNIL), CJUE C-507/17, Arrêt de la Cour (grande chambre), 24 septembre 2019.

1.20 L'Arrêt c-136/17 de 2019

Dans cette première affaire C-136/17, le litige porté devant la Commission (CNIL), puis devant le Conseil d'État, impliquait quatre demandeurs qui avaient tous enjoint Google de déréférencer les différents liens aboutissant vers des informations sensibles sur leur vie privée. Concernant le premier demandeur, GC « a demandé le déréférencement d'un lien qui renvoie à un photomontage satirique mis en ligne, sous pseudonyme, le 18 février 2011 sur YouTube » à l'occasion d'une campagne électorale « évoquant de façon explicite la relation intime » qui aurait lié la demanderesse avec le maire de la commune dont elle était directrice de cabinet¹⁹¹.

Dans le cas du second, HF « a demandé le déréférencement de lien qui renvoie à un article du quotidien Libération » relatif au suicide d'un adepte de l'Église de scientologie, le demandeur est « mentionné dans cet article en qualité de responsable des relations publiques » de ladite Église, profession qu'il a cessé d'exercer depuis lors, les faits révèlent que ce dernier aurait participé à l'article du quotidien sur sa version des faits¹⁹².

Pour BH, sa requête de déréférencement portait sur un « lien qui mène vers des articles principalement de presse, relatif à l'information judiciaire ouverte au mois de juin 1995 sur le financement du parti républicain dans le cadre de laquelle avec plusieurs hommes d'affaires et personnalités politiques, il a été mis en examen ». De plus, la procédure pénale le concernant a fini par une ordonnance de non-lieu, autrement dit un acquittement, mais malheureusement cette partie de l'issue des procédures demeure muette pour la presse¹⁹³, relativement au quatrième ED, demande que soit déréférencé le lien qui dirige l'internaute « vers deux articles publiés dans les journaux Nice-Matin et le Figaro rendant compte de correctionnelle au cours de laquelle il a été condamné à une peine sévère d'emprisonnement pour des infractions à caractères sexuels sur des mineurs. L'une de ces

¹⁹¹ CJUE, 24 septembre 2019 aff.C_136/17, *supra* note 189 au para 25.

¹⁹² *Ibid* au para 26.

¹⁹³ *Ibid* au para 27.

chroniques judiciaires mentionne, entre autres, plusieurs détails intimes relatifs à ED, qui ont été révélés à l'occasion du procès¹⁹⁴. La Cour résume bien la chronologie comme suit :

À la suite des refus opposés par Google à leurs demandes de déréférencement, les requérants au principal ont saisi la CNIL de plaintes tendant à ce qu'elle soit enjointe à cette société de procéder au déréférencement des liens en cause. Par courriers respectivement datés des 24 avril 2015, 28 août 2015, 21 mars 2016 et 9 mai 2016, la présidente de la CNIL a informé les requérants au principal de la clôture de leurs plaintes.

Les requérants au principal ont alors introduit devant la juridiction de renvoi, le Conseil d'État (France), des requêtes dirigées contre ces refus de la CNIL de mettre en demeure Google de procéder aux déréférencements demandés. Ces requêtes ont été jointes par la juridiction de renvoi¹⁹⁵.

Considérant que lesdites demandes soulèvent plusieurs questions d'interprétation de la Directive 95/46/UE, « le Conseil d'État a décidé de surseoir » les procédures avant de statuer et d'interroger la Cour de justice de l'Union européenne sur l'applicabilité des exceptions et restrictions imposées par ladite directive au traitement des données sensibles à l'exploitant d'un moteur de recherche¹⁹⁶. Pour répondre à cette première question, la CJUE commence par rappeler, « d'une part, que l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de « traitement de données à caractère personnel », au sens de l'article 2, sous b), de la Directive 95/46, lorsque ces informations contiennent des données à caractère personnel et, d'autre part, que l'exploitant de ce moteur de recherche doit être considéré comme le « responsable » dudit traitement, au sens de l'article 2, sous d), de cette directive. En effet, le traitement de données à caractère personnel effectué dans le cadre de l'activité d'un moteur de recherche se distingue et s'ajoute à celui effectué par les éditeurs de sites Web, consistant à faire figurer ces données sur une page Web, et cette activité joue un rôle décisif dans la diffusion globale desdites données en ce qu'elle rend celles-ci accessibles à tout internaute effectuant une recherche à partir du nom de la personne concernée, y compris

¹⁹⁴ *Ibid* au para 28.

¹⁹⁵ *Ibid* aux para 29 et 30.

¹⁹⁶ *Ibid* au para 31.

aux internautes qui, autrement, n'auraient pas trouvé la page Web sur laquelle ces mêmes données sont publiées. Selon la Cour, il ressort de l'économie de ces textes que l'exploitant d'un tel moteur doit, à l'instar de tout autre responsable du traitement, assurer, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que le traitement des données à caractère personnel qu'il effectue satisfasse aux exigences, respectivement, de la Directive 95/46 ou du Règlement no 2016/679. En conséquence, compte tenu des responsabilités, des compétences et des possibilités de l'exploitant d'un moteur de recherche en tant que responsable du traitement effectué dans le cadre de l'activité de ce moteur, les interdictions et les restrictions prévues à l'article 8, a)1 et 5, de la Directive 95/46 et à l'article 10 du Règlement no 2016/679, ne peuvent s'appliquer à cet exploitant qu'en raison de ce référencement et, donc, par l'intermédiaire d'une vérification à effectuer, sous le contrôle des autorités nationales compétentes, sur la base d'une demande formée par la personne concernée. Dès lors, les dispositions de l'article 8 a) 1 et 5, de la Directive 95/46 doivent être interprétées en ce sens que l'interdiction ou les restrictions relatives au traitement des catégories particulières de données à caractère personnel, visées par ces dispositions, s'appliquent, sous réserve des exceptions prévues par cette directive, également à l'exploitant d'un moteur de recherche dans le cadre de ses responsabilités de ses compétences et de ses possibilités en tant que responsable du traitement effectué lors de l'activité de ce moteur, à la suite d'une demande introduite par la personne concernée »¹⁹⁷.

Une fois la première question ainsi répondue, la Cour s'avance subséquentement à clarifier la mise en œuvre du déréférencement des liens vers les sites Internet comportant des données sensibles. Après avoir soupesé l'ensemble des considérations de la présente affaire, la CJUE convient de répondre comme suit : Les dispositions de l'article 8, paragraphes 1 et 5, de la Directive 95/46 doivent être interprétées en ce sens qu'en vertu de celles-ci, l'exploitant d'un moteur de recherche est en principe obligé, sous réserve des exceptions prévues par cette directive, de faire droit aux demandes de déréférencement portant sur des liens menant vers des pages Web sur lesquelles figurent des données à

¹⁹⁷ *Ibid* au para 35 à 48.

caractère personnel qui relèvent des catégories particulières visées par ces dispositions. L'article 8, paragraphe 2, sous e), de la Directive 95/46 doit être interprété en ce sens que, en application de celui-ci, un tel exploitant peut refuser de faire droit à une demande de déréférencement lorsqu'il constate que les liens en cause mènent vers des contenus comportant des données à caractère personnel qui relèvent des catégories particulières visées à cet article 8, paragraphe 1, mais dont le traitement est couvert par l'exception prévue audit article 8, paragraphe 2, sous e), à condition que ce traitement réponde à l'ensemble des autres conditions de licéité posées par cette directive et à moins que la personne concernée n'ait, en vertu de l'article 14, premier alinéa, sous a), de ladite directive, le droit de s'opposer audit traitement pour des raisons prépondérantes et légitimes tenant à sa situation particulière.

Les dispositions de la Directive 95/46 doivent être interprétées en ce sens que, lorsque l'exploitant d'un moteur de recherche est saisi d'une demande de déréférencement portant sur un lien vers une page Web sur laquelle des données à caractère personnel relevant des catégories particulières visées à l'article 8, paragraphe 1 ou 5, de cette directive sont publiées, cet exploitant doit, sur la base de tous les éléments pertinents du cas d'espèce et compte tenu de la gravité de l'ingérence dans les droits fondamentaux de la personne concernée au respect de la vie privée et à la protection des données à caractère personnel, consacrées aux articles 7 et 8 de la Charte, vérifier, au titre des motifs d'intérêt public importants visés à l'article 8, paragraphe 4, de ladite directive et dans le respect des conditions prévues à cette dernière disposition, si l'inclusion de ce lien dans la liste de résultats, qui est affichée à la suite d'une recherche effectuée à partir du nom de cette personne, s'avère strictement nécessaire pour protéger à la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page Web au moyen d'une telle recherche, consacrée à l'article 11 de la Charte¹⁹⁸.

On remarque ici, le souci de la Cour par l'affirmation des critères d'interprétation, la nécessité d'atteindre un juste équilibre entre les droits fondamentaux de l'Union européenne applicable, compte tenu particulièrement de la nature des données en cause et

¹⁹⁸ *Ibid* au para 69.

de sa sensibilité pour la vie privée de la personne, ainsi que de l'intérêt du public à avoir accès et en disposer de ces données, cette dernière proposition peut varier, notamment, en fonction du statut public de la personne concernée¹⁹⁹.

Pour finir, la CJUE devait également adresser la question relative à l'obligation de l'exploitant d'un moteur de recherche de tenir les liens Internet menant vers des pages Web faisant état d'informations à caractère judiciaire. Souvenons-nous du cas de ED de la présente affaire. À cet égard, la Cour s'interroge et convient que les dispositions de la Directive 95/46/UE doivent être interprétées en ce sens que, d'une part, les informations relatives à une procédure judiciaire dont une personne physique a été l'objet ainsi que, le cas échéant, celle relative à la condamnation qui en a découlé constitue des données relatives aux « infractions » et aux « condamnations pénales », au sens de l'article 8, paragraphe 5, de cette directive, et d'autre part, l'exploitant d'un moteur de recherche est tenu de faire droit à une demande de déréférencement portant sur des liens vers des pages Web, sur lesquelles figurent de telles informations, lorsque ces informations se rapportent à une étape antérieure de la procédure judiciaire en cause et ne correspondent plus, compte tenu du déroulement de celle-ci, à la situation actuelle, dans la mesure où il est constaté, dans le cadre de la vérification des motifs d'intérêt public importants visés à l'article 8, paragraphe 4, de ladite directive, que, eu égard à l'ensemble des circonstances de l'espèce, les droits fondamentaux de la personne concernée, garantis par les articles 7 et 8 de la Charte, prévalent sur ceux des internautes potentiellement intéressés, protégés par l'article 11 de la Charte²⁰⁰.

Là encore, la Cour se référant à la jurisprudence européenne affirme la nécessité de rechercher un juste équilibre entre les droits fondamentaux à savoir, la liberté d'information et de l'autre, le droit à la vie privée de la personne intéressée²⁰¹.

¹⁹⁹ *Ibid* aux para 53-57.

²⁰⁰ *Ibid* au para 79.

²⁰¹ *Ibid* au para 76.

Il en résulte selon la CJUE qu'il appartient ainsi à l'exploitant d'un moteur de recherche d'apprécier, dans le cadre d'une demande de déréférencement portant sur des liens vers des pages Web sur lesquelles sont publiées des informations relatives à une procédure judiciaire en matière pénale menée contre la personne concernée, qui se rapportent à une étape antérieure de cette procédure et ne correspondent plus à la situation actuelle, si, eu égard à l'ensemble des circonstances de l'espèce, telles que notamment la nature et la gravité de l'infraction en question, le déroulement et l'issue de ladite procédure, le temps écoulé, le rôle joué par cette personne dans la vie publique et son comportement dans le passé, l'intérêt du public au moment de la demande, le contenu et la forme de la publication ainsi que les répercussions de celle-ci pour ladite personne, cette dernière a droit à ce que les informations en question ne soient plus, au stade actuel, lié à son nom par une liste de résultats, affichée à la suite d'une recherche effectuée à partir de ce nom²⁰².

Dans sa réflexion, la Cour détermine une précision supplémentaire importante que, quand bien même l'exploitant d'un moteur de recherche devrait constater que tel n'est pas le cas en raison du fait que l'inclusion du lien en cause s'avère strictement nécessaire pour concilier les droits au respect de la vie privée et à la protection des données de la personne concernée avec la liberté d'information des internautes potentiellement intéressés, cet exploitant est, en tout état de cause, tenu au plus tard à l'occasion de la demande de déréférencement, d'aménager la liste de résultats de telle sorte que l'image globale qui en résulte pour l'internaute reflète la situation judiciaire actuelle. Ce qui nécessite notamment que des liens vers des pages Web comportant des informations à ce sujet apparaissent en premier lieu sur cette liste²⁰³.

En conséquence de ce qui précède, la CJUE statue en faveur de l'application des dispositions des articles 8 du paragraphe 1 et 5 de la Directive 95/46/UE, reprises, avec

²⁰² *Ibid* au para 77.

²⁰³ *Ibid* au para 78.

quelques modifications aux articles 9, paragraphes 1 et 10 du (RGPD) et apporte des précisions importantes, mais en somme toutes nuancées sur la portée du droit à l'oubli²⁰⁴.

1.21 La portée territoriale du droit à l'oubli

1.21.1 L'arrêt c-507/17 de 2019

Dans le second arrêt l'affaire C-507/17²⁰⁵ sur la portée territoriale du droit au déréférencement porté devant le Conseil d'État, concernait une affaire dans laquelle la Commission nationale de l'information et des libertés (CNIL) avait demandé à Google, par voie de mise en demeure, d'appliquer la désindexation demandée par une personne physique tendant à la suppression de la liste de résultats, affichée à la suite d'une recherche effectuée à partir de son nom, de liens menant vers des pages Internet, comme cela devrait se faire en conformité des exigences de la législation de l'Union européenne, mais cette fois la CNIL commandait au nom de la plaignante d'appliquer cette suppression sur toutes les extensions de nom de domaine de son moteur de recherche²⁰⁶. Google avait refusé de donner à la suite de la demeure formelle, se bornant à supprimer les liens en question des seuls résultats affichés en réponse à des recherches faites depuis les versions des États membres de l'Union européenne de son moteur de recherche. En fait, Google refuse son obligation de traitement de données à caractère personnel à l'extérieur du territoire de l'Union européenne. La Commission nationale de l'information et des libertés estime insuffisante la proposition de Google pour tenter de régler leur différend (il était question de géoblocage)²⁰⁷ et constatant que Google ne s'était pas, dans les délais impartis, conformé

²⁰⁴ *Ibid* au para 67. S'ajoute le fait que, dans l'hypothèse où le traitement porte sur les catégories particulières de données visées à l'article 8, paragraphes 1 et 5, de la directive 95/46 ou à l'article 9, paragraphe 1, et à l'article 10 du règlement 2016/679, l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel de la personne concernée est, ainsi qu'il a été relevé au point 44 du présent arrêt, susceptible d'être particulièrement grave en raison de la sensibilité de ces données.

²⁰⁵ Arrêt de la Cour (grande chambre), 24 septembre 2019, *supra* note 190

²⁰⁶ *Ibid* au para 18.

²⁰⁷ *Ibid* aux para 19-20.

à la mise en demeure avec préjudice, la CNIL après délibération en date du 10 mars 2016, a prononcé à l'égard de Google une sanction rendue publique de 100 000 euros²⁰⁸.

Par requête introduite devant le Conseil d'État français²⁰⁹, Google demande l'annulation de cette décision de la CNIL. Dans le cadre de cette procédure, le Conseil d'État a décidé de surseoir à statuer et à préférer saisir la Cour de justice de l'Union européenne sur la portée territoriale du déréférencement. De manière plus précise, la Cour devait s'interroger sur l'interprétation de la Directive 95/46/CE et répondre aux questions suivantes : « Le « droit au déréférencement », tel qu'il a été consacré par la [Cour] dans son arrêt [Google Spain et Google (6)], doit-il être interprété en ce sens que l'exploitant d'un moteur de recherche est tenu, lorsqu'il fait droit à une demande de déréférencement, d'opérer ce déréférencement sur l'ensemble des noms de domaine de son moteur, de telle sorte que les liens litigieux n'apparaissent plus quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée, y compris hors du champ d'application territorial de la Directive [95/46] ?

En cas de réponse négative à cette première question, le « droit au déréférencement », tel que consacré par la [Cour] dans son arrêt précité, doit-il être en ce sens que l'exploitant d'un moteur de recherche est seulement tenu, lorsqu'il fait droit à une demande de déréférencement, de supprimer les liens litigieux des résultats affichés à la suite d'une

²⁰⁸ *Ibid* au para 21.

²⁰⁹ En France, le Conseil d'État est la juridiction la plus élevée dans la hiérarchie administrative. Ses attributions sont à la fois juridictionnelles (tribunal), administratives et de conseil. Attributions juridictionnelles : Le Conseil d'État en appel ou en cassation sur les décisions des juridictions administratives, notamment sur les recours pour excès de pouvoir et sur les recours en interprétation et en appréciation de la légalité des actes. Il juge également en appel les jugements des tribunaux administratifs en matière d'élections communales et départementales. Ses décisions s'imposent en dernier ressort. Attributions administratives et de conseil : En vertu de la Constitution (article 38 et 39) le pouvoir exécutif doit demander l'avis du Conseil d'État sur tous les projets de Loi et d'ordonnance, ainsi que sur une grande partie des actes réglementaires et des décrets. L'avis du Conseil d'État ne s'impose pas au gouvernement. Cependant il est difficile à ce dernier d'aller à l'encontre des avis du Conseil d'État qui est au sommet de la juridiction administrative. Créé par la Constitution de l'an VIII (déc. 1799), le Conseil d'État a été réorganisé en 1872 et siège au Palais Royal (Paris 1^{er}). Constitué en sections (intérieur, finances, travaux publics, social, administration, contentieux, rapports et études), il comprend 300 membres dont les deux tiers sont présents au Palais-Royal, assistés par 390 agents. Voir Assemblée nationale, « Fiche de synthèse n°7 : Le Conseil d'État » (21 juillet 2022) en ligne : <<https://www2.assemblee-nationale.fr/decouvrir-l-assemblee/role-et-pouvoirs-de-l-assemblee-nationale/les-institutions-francaises-generalites/le-conseil-d-etat>>

recherche effectuée à partir du nom du demandeur sur le nom de domaine correspondant à l'État où la demande est réputée avoir été effectuée ou, plus généralement, sur les noms de domaine du moteur de recherche qui correspondent aux extensions nationales de ce moteur pour l'ensemble des États membres de l'Union européenne ?

En outre, en complément de l'obligation évoquée [à la deuxième question], le « droit au déréférencement », tel que consacré par la [Cour] dans son arrêt précité, doit-il être interprété en ce sens que l'exploitant d'un moteur de recherche faisant droit à une demande de déréférencement est tenu de supprimer, par la technique dite du « géoblocage », depuis une adresse IP réputée localisée dans l'État de résidence du bénéficiaire du « droit au déréférencement », les résultats litigieux des recherches effectuées à partir de son nom, ou même, plus généralement, depuis une adresse IP réputée localisée dans l'un des États membres soumis à la Directive 95/46, ce indépendamment du nom de domaine utilisé par l'internaute qui effectue la recherche ²¹⁰ ? »

Pour répondre à ces questions de grande importance, tant d'un point de vue pratique que d'un point de vue plus théorique sur l'application extraterritoriale éventuelle du droit des pays européens, la CJUE commence par l'introspection présentoir de leur jurisprudence comme point de départ l'arrêt Google Spain²¹¹. « D'entrée de jeu, la Cour affirme que cet arrêt ne détermine pas la portée géographique de la mise en œuvre d'un déréférencement. Il contient néanmoins une série d'éléments, en particulier sur la question du champ d'application territoriale de la Directive 95/46/UE »²¹². À cet égard, la Cour reconnaît qu'un déréférencement opéré sur l'ensemble des subdivisions d'un moteur de recherche serait de nature entièrement l'objectif de la directive ci-haut mentionnée et le Règlement 2016/679/UE (RGPD) qui est de garantir le haut degré de protection des données à caractère personnel dans l'ensemble du territoire de l'Union européenne²¹³. La Cour estime ensuite qu'il n'existe pas pour l'exploitant de moteur de recherche d'obligation découlant

²¹⁰ Arrêt de la Cour (grande chambre), 24 septembre 2019, *supra* note 190 au para 28.

²¹¹ *Ibid* au para 38.

²¹² *Ibid* aux para 39 à 42.

²¹³ *Ibid* aux para 44-45.

du droit de l'Union européenne de déréférencer sur l'ensemble des versions de son moteur de recherche²¹⁴. Elle ajoute de plus ce qui suit : « Si l'on admettait un déréférencement mondial, les autorités de l'Union ne seraient pas en mesure de définir et de déterminer un droit à recevoir des informations, et encore moins de le mettre en balance avec les autres droits fondamentaux de la protection des données, et à la vie privée. D'autant plus qu'un tel intérêt du public à accéder à une information va forcément varier selon sa localisation géographique, d'un État tiers à l'autre ».²¹⁵

Avec cette dernière citation, on reconnaît la préoccupation de la CJUE d'équilibre entre le droit à la protection des données à caractère personnel qui n'est pas un droit absolu, mais doit être considéré par rapport à sa mission dans la société qui distingue et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. En conséquence, la Cour détermine que l'équilibre entre le droit au respect de la vie privée et à la protection des données personnelles d'un côté et la liberté d'information sur Internet de l'autre côté, peut recevoir des interprétations différentes et varier dans des États hors de l'Union européenne²¹⁶. À ce sujet, la CJUE émet l'hypothèse suivante :

Imaginons que, pour une raison quelconque, des pays tiers interprètent certains de leurs droits de manière à empêcher les personnes situées dans un État membre de l'Union d'accéder à une information recherchée. Il existerait un risque réel d'un nivellement vers le bas, au détriment de la liberté d'expression, à l'échelle européenne et mondiale²¹⁷.

Malgré, cet extrait, la Cour propose de répondre aux questions relatives à la juridiction de façon nuancée. Dès lors, elle estime que le législateur européen n'impose pas un déréférencement mondial, il ne l'interdit pas non plus. Ainsi, selon elle, les enjeux en cause n'exigent donc pas que les dispositions de la Directive 95/46 soient d'application au-delà du territoire de l'Union. Cela ne signifie pas pour autant que le droit de l'Union ne saurait jamais imposer à un exploitant de moteur de recherche tel que Google qu'il entreprenne des actions au niveau mondial. Je n'exclus pas qu'il puisse y avoir des situations dans

²¹⁴ *Ibid* au para 46.

²¹⁵ *Ibid* au para 60.

²¹⁶ *Ibid* au para 61.

²¹⁷ *Ibid* au para 61.

lesquelles l'intérêt de l'Union exige une application des dispositions de la Directive 95/46 au-delà du territoire de l'Union. Mais dans une situation telle que celle de la présente affaire, il n'y a pas de raison d'appliquer les dispositions de la Directive 95/46 d'une telle manière²¹⁸.

La Cour réaffirme toutefois le principe d'application minimale que la désindexation doit être effectuée sur toutes les extensions de noms de domaines de l'exploitant du moteur de recherche correspondant aux États membres de l'Union européenne.

En raison de ce qui précède, la Cour dispose que :

[l]’exploitant d’un moteur de recherche n’est pas tenu, lorsqu’il fait droit à une demande de déréférencement, d’opérer ce déréférencement sur l’ensemble des noms de domaine de son moteur de telle sorte que les liens litigieux n’apparaissent plus, quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée²¹⁹.

Considérant que la Cour propose de répondre à la première question juridictionnelle par la négative, cette dernière propose de poursuivre l'analyse en traitant ensemble des deux autres questions ci-après :

par sa deuxième question, la juridiction de renvoi cherche à savoir si l'exploitant d'un moteur de recherche est seulement tenu, lorsqu'il fait droit à une demande de déréférencement, de supprimer les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur sur le nom de domaine correspondant à l'État où la demande est réputée avoir été effectuée ou, plus généralement, sur les noms de domaine du moteur de recherche qui correspondent aux extensions nationales de ce moteur pour l'ensemble des États membres de l'Union²²⁰.

La troisième question, qui est posée « en complément » à la deuxième question, vise à établir si l'exploitant d'un moteur de recherche faisant droit à une demande de déréférencement est tenu de supprimer, par la technique dite du « géoblocage », depuis une adresse IP réputée localisée dans l'État de résidence du bénéficiaire du « droit au déréférencement », les résultats litigieux des recherches effectuées à partir de son nom, ou même, plus généralement, depuis une adresse IP réputée localisée dans l'un des États membres soumis à la Directive 95/46, ce indépendamment du nom de domaine utilisé par l'internaute qui effectue la recherche²²¹.

²¹⁸ *Ibid* au para 62.

²¹⁹ *Ibid* au para 63.

²²⁰ *Ibid* au para 65.

²²¹ *Ibid* au para 66.

Pour la question technique du « géoblocage », la CJUE choisit d'élaborer avant la première et nous citons :

le géoblocage est une technique qui limite l'accès au contenu Internet en fonction de la situation géographique de l'utilisateur. Dans un système de géoblocage, la localisation de l'utilisateur est déterminée à l'aide de techniques de géolocalisation, telles que la vérification de l'adresse IP de l'utilisateur. Le géoblocage, qui constitue une forme de censure, est réputé injustifié dans le droit du marché intérieur de l'Union où il fait l'objet, notamment, d'un règlement qui vise à empêcher des professionnels exerçant leurs activités dans un État membre de bloquer ou de limiter l'accès de clients originaires d'autres États membres désireux de réaliser des transactions transfrontalières à leurs interfaces en ligne²²².

Elle pourrait, en admettant la possibilité du géoblocage « peu importe le nom du domaine de l'exploitant du moteur de recherche utilisé » et que cette technique est un moyen de ce dernier d'assurer

dans le cadre de ses responsabilités, de ses compétences et de ses possibilités que l'activité dudit moteur satisfasse aux exigences de la Directive 95/46 pour que les garanties prévues par celle-ci puissent développer leur plein effet et qu'une protection efficace et complète des personnes concernées, notamment de leur droit au respect de leur vie privée, puisse effectivement être réalisée²²³.

La Cour indique qu'une fois qu'un

droit au déréférencement est constaté, il revient donc à l'exploitant d'un moteur de recherche de prendre toute mesure à sa disposition afin d'assurer un déréférencement efficace et complet. Cet exploitant doit entreprendre toutes les démarches qui lui sont techniquement possibles. Pour ce qui est de l'affaire au principal, cela inclut, notamment, la technique dite du « géoblocage », et ce indépendamment du nom de domaine utilisé par l'internaute qui effectue la recherche²²⁴.

²²² *Ibid* au para 71. Voir aussi le Règlement (UE) 2018/302 du Parlement européen et du Conseil, du 28 février 2018, visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) no 2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE (JO 2018, L 601, p. 1).

²²³ Arrêt de la Cour (grande chambre), 24 septembre 2019, *supra* note 190 au para 73. Dans cet extrait la CJUE fait référence à l'Arrêt du 13 mai 2014, Google Spain et Google Inc. (C-131/12, EU :C :2014 :317), point 38.

²²⁴ Arrêt de la Cour (grande chambre), 24 septembre 2019, *supra* note 190, au para 74.

Le déréférencement « doit être effectué non pas au national », mais sur l'ensemble juridictionnel de l'Union européenne »²²⁵. Après cette analyse sur la portée du droit au déréférencement, la Cour convient donc de répondre aux questions deux et trois en ces mots « que l'exploitant d'un moteur de recherche est tenu de supprimer les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur effectué dans un lieu situé dans l'Union européenne. Dans ce contexte, cet exploitant est tenu de prendre toute mesure à sa disposition afin d'assurer un déréférencement efficace et complet. Cela inclut, notamment, la technique dite du « géoblocage », depuis l'adresse IP réputée localisée dans des États membres soumis à la Directive 95/46, et ce quel que soit le nom de domaine utilisé par l'internaute qui effectue la recherche »²²⁶.

Conséquemment, les deux arrêts très importants du 24 septembre 2019 contribuent efficacement à préciser le régime du droit à l'oubli sur le territoire de l'Union européenne.

À retenir :

C'est surtout, la Cour de justice de l'Union européenne qui, pour le moment, établit les assises du droit à l'oubli numérique.

Que la mise à disposition des informations litigieuses constitue une ingérence dans l'exercice du droit à la protection et du respect de la vie privée des requérants « de l'oubli » qui, en fait, découle des principes de justice fondamentale. Mais que ces droits devraient être mis en balance avec le droit à la liberté d'expression et avec la liberté de la presse garantis également par la Loi fondamentale européenne. Cette Cour précisa que, en raison de sa nature particulière, la portée du droit à la protection de la personne concernée n'était pas délimitée à l'avance, mais qu'elle devait être appréciée en mettant le droit à l'oubli ou au déréférencement en présence puisque que ce droit des requérants est protégé par la

²²⁵ *Ibid* au para 75.

²²⁶ *Ibid* au para 78.

Charte des droits fondamentaux de l'Union européenne, notamment son article 8 et devra être interprété en ce sens.²²⁷

Ce droit à l'oubli n'est sanctionné par la Cour de justice de l'Union européenne que sur le territoire des États membres de l'Union européenne. Il ne peut y avoir de demande de déréférencement à l'échelle mondiale. « En ce sens, que l'exploitant d'un moteur de recherche n'est pas tenu lorsqu'il fait droit à une demande de déréférencement, d'opérer ce déréférencement sur l'ensemble des noms de domaine de son moteur » de recherche de manière que les liens litigieux n'apparaissent plus quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée »²²⁸.

D'autre part, « l'exploitant d'un moteur de recherche est tenu de supprimer les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir du numéro du demandeur effectué dans un lieu situé dans l'Union européenne. Dans ce contexte, cet exploitant est tenu de prendre toute mesure à sa disposition afin d'assurer un déréférencement efficace et complet »²²⁹.

Cependant, la CJUE a ouvert la porte à l'éventualité d'un droit à l'oubli mondial dans certaines circonstances particulières. Dans ce cas, la Cour précise que le régime a appliqué pour les données dites sensibles, par exemple l'appartenance ou l'orientation sexuelle, l'ethnie et la religion, etc.²³⁰

En pratique, l'exploitant d'un moteur de recherche ne peut, sauf à faire des enquêtes sur tout en ce bas monde, trier de telles informations et s'assurer de leur neutralité ou véracité.

²²⁷ Charte des droits fondamentaux de l'Union européenne, *supra* note 97. Proclamée une première fois à Nice le 7 décembre 2000, la Charte des droits fondamentaux a été adoptée dans sa version définitive par les présidents de la Commission européenne, du Parlement européen et du Conseil de l'UE le 12 décembre 2007. Elle est ensuite devenue contraignante juridiquement avec la ratification du traité de Lisbonne. Selon l'article 8 : « Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la Loi ».

²²⁸ CJUE, 24 septembre 2019 aff.C_136/17, *supra* note 189.

²²⁹ Arrêt de la Cour (grande chambre), 24 septembre 2019, *supra* note 190 au para 79.

²³⁰ *Ibid.*

Mais il peut identifier le caractère potentiellement sensible de telles données. La CJUE a tranché en faveur du droit des personnes à demander le déréférencement de telles données mis en faveur de la possibilité pour l'exploitant de recherche de signaler qu'il peut s'y opposer pour cause de droit à l'information (sous le contrôle du juge si celui-ci est saisi)²³¹.

Il ressort de l'ensemble de la jurisprudence précitée, un régime assez bien défini spécifique au renforcement du droit à l'oubli sous la législation de l'Union européenne. Les personnes concernées peuvent ainsi obtenir sur demande et dans les meilleurs délais, l'effacement de toutes les données personnelles collectées lorsqu'elles cadrent dans ce régime. En cas d'inaction de la part du responsable du traitement, notamment les exploitants du moteur de recherche, elles peuvent saisir l'autorité de contrôle de l'État membre de l'Union européenne dont elle relève²³².

1.22 Sanction pour le non-respect du droit à l'oubli en Europe

La question des sanctions de l'inexécution des obligations du responsable du traitement des données a fait l'objet d'une importante évolution jurisprudentielle en Europe. Ce qui suit présente un aperçu de la jurisprudence récente quant aux sanctions imposées par les États membres de l'Union européenne.

L'objectif premier de ces sanctions est de faire respecter le Règlement général sur la protection des données (RGPD) considérant que ce « Règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données »²³³.

Et que ce Règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union européenne, que le traitement ait lieu ou non dans

²³¹ CJUE, 24 septembre 2019 aff.C_136/17, *supra* note 189, au para 67 et -78.

²³² *Ibid* au para 12. La Cour fait référence à l'article 28 de la directive 95/46 UE intitulé « Autorité de contrôle » de chaque état membre.

²³³ Règlement (UE) 2016/679, *supra* note 72 à l'article 1.a.1.

l'Union européenne²³⁴. Considérant l'ambitieuse mission du RGPD, les tribunaux européens devaient donc sévir contre les délinquants.

1.23 Condamnation de Google à 50 millions d'euros

Dans l'affaire : Délibération SAN-2019-001 du 21 janvier 2019, le 21 janvier 2019, la Commission nationale de l'information et des libertés (CNIL)²³⁵ avait prononcé cette sanction de 50 millions d'euros contre la filiale du groupe Alphabet Inc. (une entreprise, créée en 2015 comme un conglomérat de sociétés précédemment détenues par la société Google) qui est d'ailleurs identifiée au jugement comme société x²³⁶. Cette dernière fut donc condamnée pour plusieurs manquements aux règles en vigueur à savoir le RGPFD en matière de protection de données à caractère personnel des utilisateurs de son système d'exploitation pour terminaux mobiles (Android). La CNIL a fait la preuve que Google ne respecte pas certaines obligations qui émanent du droit européen sur le traitement des données personnelles, notamment le manque d'information de l'entreprise à leurs clients utilisateurs de son système Android, de l'usage qui est fait de leurs données personnelles²³⁷.

Dans cette affaire, Google a tenté par toutes les façons de faire annuler cette amende²³⁸. En définitive, il s'agissait de la première cause à faire pleinement usage du pouvoir de sanction

²³⁴ *Ibid* article 3.q.1.

²³⁵ La CNIL, ou Commission Nationale de l'informatique et des libertés est l'autorité française de protection des données. Son rôle est de s'assurer que l'informatique soit utilisée en France de manière éthique. Plus précisément, elle veille à ce que cette technologie soit au service du citoyen plutôt qu'à ce qu'elle lui nuise. Elle prête aussi attention à ce que l'informatique ne porte pas atteinte aux droits de l'homme, aux libertés individuelles ou publiques, ou à la vie privée. Depuis l'entrée en vigueur du RGPD dans européenne, la CNIL est aussi chargée de faire respecter ce règlement de protection des données. Dans le cas contraire, elle est en mesure d'infliger de lourdes amendes. Les missions de la CNIL, en ligne : <https://www.cnil.fr/fr/les-missions-de-la-cnil> (consulté le 15 août 2022).

²³⁶ Délibération SAN-2019-001 du 21 janvier 2019. Commission Nationale de l'Informatique et des libertés réunis en sa formation restreinte de délibération, 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société x, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001_21-01-2019.pdf> (consulté le 15 août 2022).

²³⁷ *Ibid* page 2.

²³⁸ La société soutient tout d'abord que la CNIL n'est pas compétente pour mener cette procédure et qu'elle aurait dû transmettre les plaintes reçues à l'autorité de protection des données irlandaise (Data Protection Commission, ci-après DPC) à laquelle il appartiendrait, en tant qu'autorité chef de file de [...], de traiter ces plaintes portant sur des traitements transfrontaliers, et ce conformément à la procédure de coopération établie à l'article 60 du RGPD. La société considère en effet que la société X doit être considérée comme son

prévue par le Règlement (UE) 2016/679 à son article 83 qui stipule notamment que « chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour violation du présent règlement [...] soient, dans chaque cas, effectives, proportionnées et dissuasives »²³⁹. Conformément à ce pouvoir, la Commission nationale de l'informatique et des libertés souligne le caractère continu et grave des infractions, tout en précisant que Google « dispose d'opération de combinaisons au potentiel quasi illimitée permettant un traitement massif intrusif des données des utilisateurs »²⁴⁰. Il est également tenu compte de la place prépondérante occupée par Google sur le marché des systèmes d'exploitation, de la gravité des manquements et de l'intérêt que représente cette décision pour l'information du public²⁴¹. En conséquence de ce qui précède, la CNIL, après avoir délibéré, décide de prononcer à l'encontre de la société X (Google) une sanction pécuniaire d'un montant de cinquante millions d'euros²⁴². La sanction représente 0,05 % du chiffre d'affaires de l'entreprise et environ 1 % de l'amende maximale que permet le RGPD²⁴³. Peu après cette décision, la société Google LLC demande au Conseil d'État, qui est la plus haute juridiction administrative française, d'annuler la présente décision et la sanction imposée par la CNIL²⁴⁴.

Le conseil d'État qui agit ici comme juge d'appel a méthodiquement rejeté les arguments du géant américain Google et confirme de ce fait la décision et la sanction issue de la délibération du 21 janvier 2019 de la Commission nationale de l'informatique et des libertés. Le Conseil d'État statuant en ces mots : « il résulte de ce qui précède qu'eu égard

établissement principal au sein de l'Union européenne pour certains des traitements transfrontaliers qu'elle met en œuvre, et notamment ceux objets des plaintes reçues par la CNIL. Par conséquent, l'autorité de protection des données devrait selon elle être regardée comme son autorité de contrôle chef de file et être chargée, à ce titre, de traiter les plaintes reçues par la CNIL. Voir aussi : *Supra* note 236, à la p 3.

²³⁹ Règlement (UE) 2016/679, *supra* note 72 à l'article 83.

²⁴⁰ Délibération SAN-2019-001 du 21 janvier 2019, *supra* note 236 à la p 15.

²⁴¹ *Ibid* à la p 16.

²⁴² *Ibid* à la p 16, conclusion.

²⁴³ Règlement (UE) 2016/679, *supra* note 72 à l'article 83 et Délibération SAN-2019-001 du 21 janvier 2019, *supra* note 236.

²⁴⁴ Conseil d'État statuant au contentieux CR. No 430810. Société Google LLC, Séance du 12 juin 2020.

Lecture du 19 juin 2020. Sanction infligée à Google par la CNIL. République Française au nom du peuple français.

à la gravité particulière des manquements commis, qui tient à la nature des exigences méconnues et à leurs effets sur les utilisateurs, au caractère continu de ces manquements et à la durée de la période durant laquelle ils ont perduré, aux plafonds prévus par le paragraphe 4 de l'article 83 du RGPD, et à la situation financière de la société, la sanction pécuniaire de 50 000 000 d'euros prononcée à l'encontre de la société Google ne revêt pas un caractère disproportionné. Il résulte de tout ce qui précède, sans qu'il soit besoin de poser des questions préjudicielles à la Cour de justice de l'Union européenne, que la requête de la société Google LLC doit être rejetée »²⁴⁵.

Comme on peut l'avancer, la CNIL devient ainsi la première instance de régulation européenne à sanctionner une plateforme Internet mondiale en utilisant les dispositions du règlement européen sur la protection des données personnelles (RGPD). Ce qui ressort d'important, c'est l'application effective du règlement par la CNIL et des principes déclarés dans cette affaire que les manquements constatés privent les utilisateurs de garanties fondamentales concernant des traitements pouvant porter atteinte à leur vie privée²⁴⁶.

1.24 Amende historique pour le non-respect du droit à l'oubli

Dans le dossier : Dos-2019-03780, Autorité de protection des données. *X c. Google* (déréférencement/droit à l'oubli), le 14 juillet 2020, la Chambre contentieuse de l'autorité de protection des données en France a sanctionné Google Belgium pour le non-respect du droit à l'oubli demandé par un citoyen belge à une amende record de 600 000 euros. Il s'agit d'une décision historique pour la protection des données personnelles²⁴⁷.

En substance, le plaignant dont l'identité n'a pas été révélée, mais présentée dans la décision comme une personnalité publique reproche à Google Belgium son refus de faire droit à ses demandes de déréférencement et de suppression d'informations personnelles.

²⁴⁵ *Ibid* à la p 15.

²⁴⁶ Délibération SAN-2019-001 du 21 janvier 2019, *supra* note 236 à la p 16.

²⁴⁷ Chambre contentieuse, Décision quant au fond 37/2020 du 14 juillet 2020, Belgique. No. De dossier : Dos -2019-03780, Autorité de protection des données. *X C. Google* (déréférencement/droit à l'oubli), en ligne : <<https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf>>

Alors que selon le plaignant, « une recherche effectuée sur la base de son nom et prénom entraîne le référencement de contenus attentatoires à son honneur et à sa réputation dans la presse écrite belge »²⁴⁸. Une partie des pages Internet qu'il souhaitait ainsi voir déréférencer, en plus d'être obsolète concerne une allégeance politique, que celui-ci réfute et pour la seconde partie est relative à une plainte pour harcèlement à son encontre, déclarée non fondée, il y a plusieurs années²⁴⁹. Google a donc refusé purement et simplement de ne pas déréférencer les liens vers les pages Internet litigieuses²⁵⁰.

La décision de l'Autorité de protection des données (APD) Belge, relativement aux pages Internet concernant l'allégeance politique, la Chambre contentieuse de l'APD a considéré que vu le rôle du plaignant dans la vie publique et au fait que l'étiquetage politique constitue une information liée à la transparence dans la désignation du cadre général de l'exercice des mandats dans la fonction publique (sujet au cœur du débat démocratique et qui a vocation à être étudié au cours du temps) et dès lors que dans le présent contexte, la mention de son étiquetage ne révèle aucune de ses opinions politiques », dans ces circonstances spécifiques à l'affaire, la Chambre contentieuse considère que le référencement est nécessaire à l'exercice du droit à la liberté d'expression et d'information et que, par conséquent, en application de l'article 17,3 a) du RGPD, « c'est à bon droit que Google l'a maintenu »²⁵¹ et a ainsi donné raison à Google.

Quant aux âges Internet concernant une plainte à l'encontre du demandeur-plaignant, l'APD estime que la demande de déréférencement est bien fondée pour les raisons suivantes.

La Chambre contentieuse considère par conséquent que dès réception du formulaire de demande de déréférencement introduit par le plaignant, Google a eu une connaissance effective du caractère ancien de la plainte pour harcèlement, du fait que cette information n'était pas mise à jour et enfin, s'agissant d'une plainte pour harcèlement, qu'elle était susceptible de porter préjudice au plaignant. Autrement dit, Google avait dès ce moment une connaissance

²⁴⁸ *Ibid* au para 2.

²⁴⁹ *Ibid* aux para 3-4.

²⁵⁰ *Ibid* au para 5-6.

²⁵¹ *Ibid* au para 145.

effective de motifs sérieux de nature à exiger un déréférencement sur base de l'article 17,1., a) du RGPD²⁵².

En décidant de refuser de déréférencer promptement, alors que Google aurait dû procéder, car elle avait une connaissance effective des motifs sérieux de la nature à justifier que le référencement ne pouvait pas être maintenu en application de l'article 17, 3., a), du RGPD, Google a également manqué aux obligations consacrées dans l'article 17,1., a), du RGPD puisque cette dernière a refusé de procéder au déréférencement de manière du moins temporaire en vue de vérifier les détails de plainte auprès du demandeur²⁵³. Ces mêmes faits, selon la Chambre contentieuse, constituent un manquement important à l'article 6,1,f), du RGPD dès lors que les circonstances de l'espèce le justifient, « les intérêts du plaignant qui exigent une protection des données à caractère personnel prévalaient sur les intérêts légitimes de Google à référencer les contenus disponibles via l'Internet »²⁵⁴.

En conséquence :

La Chambre contentieuse considère que ces manquements présentent un caractère grave de la part de Google. Bien que les dispositions violées comportent des normes ouvertes à interprétation et que le droit à la protection des données ne soit pas un droit absolu, le déréférencement est une obligation claire d'un moteur de recherche suite à l'arrêt Google Spain. Comme évoqué par la Cour de Justice, la gravité potentielle de l'ingérence est sérieuse et les droits d'une personne concernée prévalent, en principe, sur l'intérêt de ce public à trouver ladite information lors d'une recherche portant sur le nom de cette personne²⁵⁵.

Dans le cas d'espèce, Google étant parfaitement au courant de tous les éléments factuels, suite à la demande du plaignant, n'a pas agi de façon diligente par son refus de déréférencer les contenus en question, alors que le plaignant lui avait fourni la preuve de leur caractère dépassé. La Chambre contentieuse considère dans ce contexte que ces éléments sont comparables aux éléments soulignés dans le cas Google Spain, notamment ceux relatifs au caractère inadéquat et au temps écoulé. Dès lors, donner suite à la demande du plaignant ne demande pas une évaluation juridique compliquée. La Chambre contentieuse ajoute que dans ces circonstances, il n'y a aucune atteinte disproportionnée à la liberté d'expression et d'information, contrairement à ce que soutient Google Belgium SA²⁵⁶.

²⁵² *Ibid* au para 159.

²⁵³ *Ibid* au para 161.

²⁵⁴ *Ibid* au para 162.

²⁵⁵ *Ibid* au para 163.

²⁵⁶ *Ibid* para 164.

Enfin, quant à l'analyse de l'équilibre des droits et intérêts en présence, la Chambre contentieuse répond que Google a manqué aux obligations stipulées à l'article 12,1. Et 4. Du RGPD,

puisque le demandeur s'est trouvé confronté à un motif de refus de sa demande lacunaire ne lui permettant ni de connaître ni de comprendre complètement la motivation de Google. [...] En conclusion, la réponse de Google quant au motif du refus de déréférencer, a manqué de transparence et n'a pas été suffisamment compréhensible, en violation des articles 12.1. et 4 du RGPD²⁵⁷.

Et vu que le défaut de Google de déréférencer les liens litigieux est susceptible d'avoir de sérieuses répercussions pour le demandeur-plaignant, les droits et intérêts de la personne concernée doivent prévaloir²⁵⁸. La Chambre contentieuse considère qu'en fonction de l'ensemble des faits de la présente décision que Google a fait preuve de négligence et de manquement grave en refusant. À cet égard, le Président de la Chambre contentieuse de l'Autorité de protection des données qui est le signataire de la décision, Hielke Hijmans s'exprime de la façon suivante :

Dans le droit à l'oubli, il faut trouver un juste équilibre entre d'une part, le droit du public à accéder à l'information, et, d'autre part, les droits et intérêts de la personne concernée. Si certains des articles cités par le plaignant peuvent être considérés nécessaires au droit à l'information, les autres, qui relatent des faits de harcèlement non démontrés et vieux d'environ 10 ans, doivent pouvoir tomber dans l'oubli. En maintenant accessibles, via son moteur de recherche largement utilisé par les internautes, des liens qui peuvent causer d'importants dommages à la réputation du plaignant, Google a fait preuve d'une claire négligence²⁵⁹.

1.25 La sanction

D'abord la Chambre contentieuse ordonne à Google Belgium de mettre en conformité des données et à cet effet, de faire mettre en œuvre toutes mesures techniques efficaces afin de cesser les référencement aux pages Internet litigieuses pour l'ensemble des autres sites

²⁵⁷ *Ibid* para 165.

²⁵⁸ *Ibid* aux para 165-168.

²⁵⁹ Communiqués de presse : Autorité de protection des données 600 000 euros d'amende : l'APD sanctionne Google Belgium pour non-respect du droit à l'oubli, en ligne : <<https://www.autoriteprotectiondonnees.be/citoyen/600.000-euros-damende-lapd-sanctionne-google-belgium-pour-non-respect-du-droit-a-loubli>> (consulté le 15 août 2022).

Internet du moteur de recherche dans toutes leurs versions linguistiques dans l'espace économique de l'Europe, et ce dans les sept jours de la signification de la décision²⁶⁰.

En plus, de l'injonction de procéder au déréférencement, la Chambre contentieuse considère que la gravité des manquements nécessite en complément, « à des fins dissuasives l'imposition d'amendes administratives »²⁶¹. Elle souligne que

le but d'infliger une amende administrative n'est pas seulement de mettre fin à une infraction commise, mais surtout de veiller à une application efficace des règles du RGPD en cas de violations sérieuses, en complément ou à la place des mesures correctives qui sont imposées²⁶².

L'Autorité de protection des données belges a ainsi infligé à Google une amende de 600 000 euros pour ne pas avoir déréférencé les pages Internet problématiques et obsolètes à l'encontre du demandeur, pour le manque d'information obligatoire à l'égard du demandeur pour justifier le refus de déréférencement, ainsi que le manque de transparence dans le formulaire à cet effet de Google²⁶³.

1.26 Le droit à l'oubli constitue une obligation claire

Dans le cadre de cette décision, la Chambre contentieuse, sous la plume de son président Monsieur Hielke Hijmans, s'exprime en *obiter dictum* sur l'implémentation du droit à l'oubli en Europe et sur le comportement délinquant de la multinationale Google à l'égard de la règle de droit européenne comme suit :

Comme il a été souligné à plusieurs reprises, Google LLC fait l'objet d'un contentieux important en ce qui concerne la mise en œuvre du droit à l'oubli et des dispositions qui y sont liées, que ce soit en France ou encore en Suède. Force est de constater que malgré ces précédents, le *modus operandi* du groupe ne permet toujours pas à celui-ci de remplir totalement et adéquatement ses obligations nées du droit à l'oubli. Même si elle nécessite de faire une analyse au cas par cas, le droit à l'oubli constitue une obligation claire²⁶⁴.

²⁶⁰ Chambre contentieuse, Décision quant au fond 37/2020 du 14 juillet 2020, Belgique, *supra* note 247 au para 166.

²⁶¹ *Ibid* au para 167.

²⁶² *Ibid* au para 168.

²⁶³ *Ibid* aux para 175-177.

²⁶⁴ *Ibid* au para 175 (IV).

En poursuivant dans la même direction, la Chambre contentieuse décide de publier la décision à l'encontre de Google au bénéfice du public, elle s'explique :

La Chambre contentieuse précise que la publication avec identification de la partie défenderesse poursuit deux objectifs. Elle vise tout d'abord un objectif d'intérêt général, parce qu'elle explique les responsabilités (des filiales dans l'Union) de Google sous le RGPD. En effet, au vu de l'importance du moteur de recherche « Google » pour de très nombreux internautes et le fait qu'une partie importante des personnes résidant en France se trouvent référencées d'une manière ou d'une autre sur le moteur de recherche « Google », la Chambre contentieuse estime pertinent de donner à cette décision une publicité qui puisse sensibiliser les internautes aux droits qui sont les leurs en vertu du RGPD. À ce titre, même si la décision ne concerne de manière directe que le plaignant, elle est d'intérêt pour une large partie du grand public. La publication de la décision est à cet égard tout à fait pertinente²⁶⁵.

La publication de la décision vise également un effet dissuasif, considère la Chambre contentieuse²⁶⁶.

Le président de l'Autorité de protection des données belge, Monsieur David Stevens, accueille favorablement la décision de la Chambre contentieuse ainsi :

Cette décision n'est pas seulement importante pour nos citoyens belges, elle est aussi la preuve de notre ambition de mieux protéger la vie privée « en ligne » en collaboration avec nos homologues européens, ce qui demande des actions concrètes contre des acteurs actifs au niveau mondial. De cette manière, nous souhaitons contribuer activement au développement d'une réelle *culture de protection des données* au niveau européen²⁶⁷.

Comme nous l'avons vu précédemment, les personnes physiques résidentes d'un pays membre de l'Union européenne²⁶⁸ peuvent donc bénéficier du droit à l'oubli numérique

²⁶⁵ *Ibid* au para 183.

²⁶⁶ *Ibid* au para 183.

²⁶⁷ Communiqués de presse : Autorité de protection des données 600 000 euros d'amende, *supra* note 259, à la p 2.

²⁶⁸ Règlement (UE) 2016/679, *supra* note 72, art.3 (2) et (3) – Champ d'application territorial. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable

fort bien établi autant sur le plan du régime étatique applicable que sur la constante évolution de la jurisprudence. Sans négliger les fortes sanctions imposées aux délinquants.

du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées.

CHAPITRE II

L'ÉVOLUTION DU DROIT À L'OUBLI AUX ÉTATS-UNIS, CANADA ET AU QUÉBEC

Si en Europe, on tend à considérer le droit à la vie privée comme un droit fondamental surpassant la liberté d'expression, il n'en est pas de même aux États-Unis. En fait, le droit de la presse et la liberté d'expression protégés par le premier amendement de la Constitution des États-Unis à la déclaration des droits (Bill of Rights) qui furent ratifiés le 15 décembre 1791²⁶⁹ ont la primauté sur le droit à la vie privée emportant de ce fait la suppression de données à caractère personnel publiées. La jurisprudence américaine semble unanime à ce sujet²⁷⁰.

Aux États-Unis, les détracteurs au droit à l'oubli estiment que ce nouveau droit est contraire au premier amendement de la Constitution américaine, s'appuyant sur le fait que le droit à la vie privée n'est pas explicitement mentionné dans la Constitution²⁷¹.

Nonobstant cette dernière affirmation, il a été constaté que le droit à la vie privée est implicite dans les premiers, troisième, quatrième, cinquième, neuvième et quatorzième amendement de cette même constitution américaine²⁷².

Considérant, ce préambule factuel et l'approche étroite des garanties constitutionnelles américaines annoncent que les États-Unis ne disposent pas de régime permettant une protection des données à caractère personnel. Malgré l'utilisation volumineuse de données personnelles des dernières années par les grandes plateformes américaines de l'Internet,

²⁶⁹ Le premier amendement de la Constitution des États-Unis d'Amérique fait partie des dix amendements ratifiés en 1791 et connus collectivement comme la Déclaration des Droits (*Bill of Right*). Il interdit au Congrès des États-Unis d'adopter des lois limitant la liberté de religion et d'expression, la liberté de presse ou le droit à « s'assembler pacifiquement ». Voir Les amendements à la Constitution des États-Unis ratifiés par les États, La « Déclaration Des Droits », en ligne (21 juillet 2022) : <<https://www.state.gov/wp-content/uploads/2020/05/FRE-Constitution.pdf>>

²⁷⁰ Viktor and Mayer-Schoenberger, *supra* note 13 à la p 11.

²⁷¹ Timothy Zick, *Clouds, caméras et ordinateurs : le premier amendement et lieux publics den réseau*, (2007) 59 : 1 FL, L. Recueil 263

²⁷² Viktor and Mayer-Schoenberger, *supra* note 13 à la p 14.

nul besoin de nommer, donnent l'impression que les États-Unis manquent totalement de volonté d'adopter une loi ou un cadre constitutionnel convaincant pour la protection de la vie privée et la protection de ces données²⁷³.

La protection à l'égard du droit et au respect de la vie privée est reconnue au sein de la Common Law de chaque État américain et notamment dans la jurisprudence en matière de la responsabilité civile, qui est en fait le Régime applicable sur le plan du droit à la vie privée.

Aux États-Unis, le droit au respect à la vie privée est mentionné pour la première fois, à la fin du 19^e siècle, la publication de photographie dans la presse est à l'origine de ce nouveau défi pour la jeune notion de la vie privée en droit. Le développement de cette nouvelle technologie menaçait la vie privée des personnes concernées. En réaction à ce phénomène, deux distingués juristes américains, Samuel Warren et Louis Brandeis, ont publié un article dans le prestigieux *Harvard Law Review* en 1890 ayant comme titre « The right to Privacy » qui édifie les assises des règles de responsabilité civile en matière de vie privée²⁷⁴. À ce titre, nous avons le devoir moral de citer le préambule du célèbre article pour bien saisir les similarités avec le droit à l'oubli numérique: « That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave remedy only for physical interference with life and property, for trespasses vi et armis. Then the « right to life » served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, --the right to be let alone; the right to liberty secures the exercise of extensive civil privileges;

²⁷³ *Ibid* à la p 15.

²⁷⁴ Samuel Warren, "Louis Brandeis, the right to privacy", (1890) 4 *Harvard Law* 193

and the term « property » has grown to comprise every form of possession – intangible, as well as tangible »²⁷⁵.

L'ensemble de la jurisprudence sur la responsabilité civile américaine appelée « privacy torts », ces règles juridiques protègent notamment contre des atteintes relevant de la sphère de vie privée, incluant les photographies et les publications sans le consentement de personnes intéressées²⁷⁶.

2.1 L'ÉVOLUTION AUX ÉTAS-UNIS

2.1.1 Privacy Act de 1974

Outre ces principes de la Common Law développés au niveau de chaque État au cours des années, les Américains disent des lois fédérales se rapportent à la protection des données à caractère personnel dans certains domaines. Le Privacy Act de 1974 est la première Loi sur la protection et le traitement des données à caractère personnel effectuée par le gouvernement fédéral²⁷⁷. En substance, cette Loi instaure des règles à suivre sur le traitement des données personnelles collectées par les différents départements étatiques du gouvernement américain. Elle établit un code de pratiques équitables en matière d'information qui régit la collecte, la maintenance, l'utilisation et la diffusion des

²⁷⁵ *Ibid* à la p 193 : Que l'individu jouisse d'une pleine protection en sa personne et dans ses biens est un principe aussi ancien que la Common Law ; mais il s'est avéré nécessaire de définir à nouveau de temps à autre la nature exacte et l'étendu de cette protection. Les changements politiques, sociaux et économiques entraînent la reconnaissance de nouveaux droits et la Common Law, dans son éternelle jeunesse, grandit pour répondre aux nouvelles exigences de la société. Ainsi, dans les temps les plus reculés, la Loi n'offrait de recours que pour les atteintes physiques à la vie et à la propriété, pour les atteintes vie et amis. Alors le « droit à la vie » ne servait qu'à protéger le sujet des coups et blessures sous ses diverses formes ; la liberté signifiait la liberté de toute contrainte réelle ; et le droit de propriété garantissait à l'individu ses terres et son bétail. Plus tard, vint la reconnaissance de la nature spirituelle de l'homme, de ses sentiments et de son intellect. Peu à peu, la portée de ces droits légaux s'est élargie ; et maintenant le droit à la vie en est venu à signifier le droit de jouir de la vie, -- le droit d'être laissé tranquille ; le droit à la liberté garantit l'exercice de privilèges civils étendus ; et le terme « propriété » s'est développé pour englober toutes les formes de possession – intangibles aussi bien que tangibles [Notre traduction].

²⁷⁶ William Lloyd Prasser, "Privacy", (1960) 48 Cal L Rev 1960, p. 383.

²⁷⁷ Privacy of 1974, as amended, 5 U.S.C. 552A., en ligne: [justice.gov/opcl/privacy-act-1974](https://www.justice.gov/opcl/privacy-act-1974).

informations sur les individus concernés dans les systèmes informatiques d'enregistrement par les agences fédérales²⁷⁸.

La Loi sur la protection des renseignements personnels exige que l'organisme donne au public un avis de leurs dossiers par publication dans le Registre fédéral et interdit la divulgation d'un dossier concernant une personne à partir d'un système informatique de dossier, sans le consentement écrit de la personne à moins que la divulgation ne soit conforme à l'une des douze (12) exceptions²⁷⁹. Considérant le champ d'action très limité, en plus des nombreuses exceptions, cette Loi met en œuvre un semblant de protection des données qui avait été développé dans le cadre limitatif du ministère de la Santé américaine en 1973, l'adaptation pour les données personnelles civiles n'est pas des plus désignée ou heureuse dans le contexte actuel²⁸⁰.

Après le Privacy Act de 1974, le législateur américain a progressé en développant des lois visant la protection des données à caractère personnel dans le secteur privé, parmi elles on a retrouvé les plus importantes : *Health Insurance Portability and Accountability Act 1996*, visant la protection des données en santé²⁸¹ ; *Gramm-Leach-Bliley Act 1999*, visant la protection de données financières²⁸² ; *Children's Online Privacy Protection Act 1998* ; visant la protection des données concernant les enfants²⁸³ ; *Electronic Communication*

²⁷⁸ *Ibid.*

²⁷⁹ *Ibid.*

²⁸⁰ Privacy Act 1974, Overview, Edition 2020, The United States department of justice, en ligne: <justice.gov/opcl/overview-privacy-act-1974-2020-edition>.

²⁸¹ Health Insurance Portability and Accountability Act of 1996 (HIPAA). Public Law 104-191. La Health Insurance Profitabilité and Accountability Act de 1996 (HIPAA) et une loi fédérale qui exige la création de normes nationales pour protéger les informations sensibles sur la santé des patients contre la divulgation sans le consentement ou la connaissance du patient. Le département américain de la Santé et des Services sociaux (HHS) a publié la règle de confidentialité HIPAA pour mettre en œuvre les exigences de la Loi HIPAA. La règle de sécurité HIPAA protège un sous-ensemble d'informations couvertes par la règle de confidentialité, En ligne : <<https://www.hhs.gov/hipaa/for-professionals/index.html>>.

²⁸² Gramm_Leach_Bliley Act., NOV. 12, 1999, Public Law 106-102. La Loi Gramm-Leach-Bliley oblige les institutions financières – les entreprises qui proposent aux consommateurs des produits ou services financiers tels que des prêts, des conseils financiers ou d'investissement ou des assurances – à expliquer leurs pratiques de partage d'informations à leurs clients et à protéger les données sensibles; disponible en ligne : <<https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>>

²⁸³ Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505. La COPPA impose certaines exigences aux opérateurs de sites Web ou de services en ligne destinés aux enfants de moins de 13 ans, ainsi

Privacy Act 1986 ; visant la protection des données de télécommunications²⁸⁴. On remarque que ces lois américaines sont protectrices envers les données à caractère personnel dans le secteur privé de façon ciblée et d'applications très restreintes. Sans oublier que ces droits devront être interprétés par les tribunaux dans un contexte constitutionnellement américain qui se limite aux actions gouvernementales et non l'action privée. Même si au mieux la réinterprétation constitutionnelle, on peut limiter la collecte et le traitement des données personnelles par le gouvernement, mais dans la réalité rapprocher cela n'aura aucune incidence sur la pratique du secteur privé²⁸⁵. Pour le présent, aux États-Unis, l'inaction législative sur la protection des données à caractère personnel semble convenir. Les apparences donnent à penser qu'il n'y a pas de volonté de la majorité d'adopter une loi pour la protection et le traitement des données personnelles par le gouvernement américain ni d'argument normatif des tribunaux pour qu'il statue sur les revendications pertinentes d'ordre constitutionnel²⁸⁶. Même les constitutionnalistes concèdent qu'il n'y a pas de reconnaissance constitutionnelle de la protection des données personnelles et du droit à l'oubli de la société américaine²⁸⁷. Il est donc peu probable que la Cour Suprême des États-Unis trouve le moyen de réinterpréter la constitution et trouve un passage favorable inclusif du droit à l'oubli dans le cadre plus général d'une violation d'une garantie constitutionnelle

qu'aux opérateurs d'autres sites Web ou services en ligne qui ont effectivement connaissance qu'ils collectent des informations personnelles en ligne auprès d'un enfant de moins de 13 ans; en ligne : <<https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>>

²⁸⁴ Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. 2510-2523. L'ECPA, telle que modifiée, protège les communications filaires, orales et électroniques pendant que ces communications sont effectuées, sont en transit et lorsqu'elles sont stockées sur de ordinateurs. La Loi s'applique aux courriels, aux conversations téléphoniques et aux données stockées électroniquement. L'Electronic Communications Privacy Act & the Stored Wire Electronic Communications Act sont communément appelés l'Electronic Communications Privacy Act (ECPA) de 1986. Mais ne s'appliquait pas à l'interception d'ordinateurs et d'autres communications numériques et électroniques. Plusieurs textes législatifs ultérieurs, dont le USA PATRIOT ACT, clarifient et mettent à jour l'ECPA pour suivre l'évolution des nouvelles technologies et méthodes de communication, notamment en assouplissant les restrictions d'accès des forces de l'ordre aux communications stockées dans certains cas; en ligne : <<https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285>>

²⁸⁵ Viktor and Mayer-Schoenberger, *supra* note 13 à la p 14.

²⁸⁶ *Ibid* à la p 12.

²⁸⁷ *Ibid* à la p 13.

particulière²⁸⁸. Compte tenu de ce qui précède, abordons quelques exemples d'arrêts clés de la Cour suprême américaine.

2.1.2 Cox Broadcasting Corp. C. Cohn

En 1975, dans l'arrêt *Cox Broadcasting Corp. C. Cohn*²⁸⁹, la Cour suprême a décidé que la publication dans la presse du nom d'une victime d'agression sexuelle était légale. Dans cet arrêt, il s'agissait d'un journaliste de Cox Broadcasting qui a rapporté aux nouvelles que la victime d'un viol et d'un meurtre était la fille de Cohn. Il a trouvé cette information en voyant l'acte d'accusation lors du procès pénal public de l'auteur présumé. Cependant, divulguer le nom d'une victime de viol constituait un délit en Géorgie. Cohn a intenté une action qui a été chassée par la Cour suprême de Géorgie comme une plainte pour atteinte à la vie privée. Il a également statué que le droit pénal géorgien ne violait pas le premier et le quatorzième amendement.²⁹⁰

Dans le cadre d'une requête en nouvelle audition, les appelants ont soutenu que le nom d'une victime de viol était une question d'intérêt public et pouvait donc être publié en toute impunité, mais la Cour suprême de Géorgie a rejeté la requête au motif que la Loi déclarait une politique de l'État selon laquelle le nom d'une victime de viol n'était pas une question d'intérêt public et a soutenu que la Loi était une limitation légitime de la liberté d'expression du premier amendement²⁹¹.

Or, la Cour suprême des États-Unis devait répondre en appel ultime, à la question en litige suivante : la Loi géorgienne a-t-elle violé la liberté de la presse telle que protégée par le premier et le quatorzième amendement de la Constitution ?

²⁸⁸ *Ibid.*

²⁸⁹ *Cox Broadcasting Corp. c. Cohn* (1975) 42 US. 469.

²⁹⁰ *Ibid.*

²⁹¹ *Cox Broadcasting Corp. c. Cohn* (1975) 42 US. 469, *supra* note 289 à la p 476.

La Cour a estimé que la Loi géorgienne violait la Constitution. Le juge White a reconnu la primauté des questions de confidentialité et de liberté de la presse, mais il a également identifié des raisons impérieuses pour lesquelles la presse ne devrait pas être restreinte dans cette affaire. Premièrement, les médias sont une ressource importante pour les citoyens qui leur permet d'examiner attentivement les débats du gouvernement. Les commissions et le jugement des crimes sont des questions pertinentes pour l'intérêt public. Deuxièmement, dans le développement du droit à la vie privée, la Cour a statué que les intérêts de la vie privée « s'estompent » dans les cas où « des informations controversées figurent déjà dans le dossier public ». Retreindre les médias comme l'a fait la Loi géorgienne était un empiètement dangereux sur la liberté de la presse, a fait valoir White, car cela « inviterait à la timidité et à l'autocensure²⁹².

Dans cette affaire, le tribunal a été particulièrement convaincu par le fait que les actes d'accusation avaient déjà rendu l'information publique, de sorte que l'État ne pouvait raisonnablement prétendre que la presse devait la garder privée. Étant donné que l'État avait déjà démontré sa conviction que l'information était d'intérêt public en l'incluant dans les actes d'accusation, la presse avait le droit de divulguer l'identité de la victime²⁹³.

2.1.3 Oklahoma Publishing Co. c. Distric Court for Oklahoma County

Également, dans l'arrêt *Oklahoma Publishing Co. C. District Court for Oklahoma County*, la Cour suprême américaine a annulé une ordonnance interdisant à la presse de publier des informations obtenues lors d'une audience préliminaire dans le cadre d'une procédure criminelle, ouverte au public et à la presse. La Cour a conclu que l'ordonnance violait le droit à la liberté de la presse du premier amendement de la Constitution²⁹⁴.

L'affaire découlait d'une ordonnance préalable au procès d'un juge interdisant aux médias de divulguer davantage le nom d'un garçon de 11 ans accusé de meurtre, bien que son

²⁹² Rendu pour l'opinion de la majorité, le juge Byron R. White aux pp 493-495. *Ibid.*

²⁹³ *Ibid* à la p 477.

²⁹⁴ *Oklahoma Publishing Co. c. District Court for Oklahoma County*, (1977), 430 US 308.

identité ait été légalement acquise lors d'une audience publique. Le journaliste avait appris le nom du garçon lorsqu'il avait assisté à son audience de détention au tribunal pour mineurs. Alors que le garçon était escorté du palais de justice jusqu'à un véhicule, un photographe de presse l'a pris en photo. Les journaux locaux ont imprimé le nom et la photographie du garçon, et les chaînes de télévisions locales ont montré des images filmées de lui et l'ont identifié. Le juge a ensuite interdit aux médias de publier ou de diffuser le nom et la photo du garçon dans le cadre de procédures judiciaires ultérieures.

En appel par *The Daily Oklahoman*, la Cour suprême de l'Oklahoma « a conclu que la restriction de la presse était valable dans l'intérêt de la réhabilitation éventuelle du jeune délinquant et de son intégration ultérieure dans la société ». Cependant, la Cour suprême des États-Unis, dans une brève opinion *par curiam*, a jugé à l'unanimité qu'en vertu de la liberté de la presse du premier amendement, le tribunal d'État ne pouvait pas interdire « la publication d'informations largement diffusées obtenues lors de procédures judiciaires qui étaient en fait ouvertes au public²⁹⁵.

La Cour suprême des États-Unis a déclaré que sa décision était « contrainte » par ses décisions dans *Cox Broadcasting Corp. v. Cohn* (1975) et *Nebraska Press Association v. Stuart* (1976), qui restreignaient les ordonnances de bâillon contre la communication d'informations légalement acquises en audience publique ou dans des documents judiciaires publics²⁹⁶.

2.1.4 Smith c. Daily Mail Publishing Co.

Deux ans plus tard, dans *Smith v. Daily Mail Publishing Co.*²⁹⁷, la Cour suprême des États-Unis a étendu une protection similaire aux informations obtenues légalement en dehors du

²⁹⁵ *Ibid* au para 5-6.

²⁹⁶ *Ibid* au para 4.

²⁹⁷ *Smith v. Daily Mail Publishing Co.*, (1979) 443 U.S. 97.

palais de justice ou des audiences publiques, grâce à des techniques de recherche journalistique régulières.

Les faits : le 9 février 1978, des témoins oculaires ont identifié un jeune de 14 ans comme étant le présumé auteur de la fusillade et tué un élève de 15 ans dans une école secondaire. Deux journaux, le Charleston Daily Mail et le Charleston Gazette ont appris la nouvelle grâce à une surveillance de routine et d'information par les communications des bandes radio de la police. Ils ont immédiatement dépêché des journalistes et des photographes sur les lieux, où ils ont obtenu le nom du jeune auteur présumé en parlant à des témoins et à la police. Le Daily Mail n'a pas initialement rapporté le nom et sa photographie. Plusieurs stations de radio ont également diffusé son nom et le Daily Mail en a fait de même par la suite.

Les deux journaux ont été inculpés pour violation de la Loi de l'État. Ils ont contesté la Loi, affirmant qu'elle agissait comme une restriction préalable inconstitutionnelle et a obtenu une ordonnance d'interdiction de la Cour d'appel suprême de Virginie-Occidentale. L'État a répliqué que la Loi était constitutionnelle parce que l'intérêt public à protéger l'identité des mineurs l'emportait sur la forte présomption contre les restrictions antérieures²⁹⁸.

La décision de la Cour suprême des États-Unis fut unanime. Le juge en chef Warren E. Burger a rendu l'avis de la Cour et est d'opinion que la Loi de Virginie-Occidentale fonctionne comme une restriction préalable ou une sanction post-publication, elle serait soumise au même examen rigoureux et a constaté que les décisions antérieures, bien qu'elles ne soient pas décisives, « suggèrent fortement » que si un journal obtient légalement des informations véridiques sur une question d'importance publique, un État ne peut pas constitutionnellement punir la publication, sauf pour servir un intérêt de l'État « de premier ordre ».

²⁹⁸ *Ibid.*

Le fait que les journaux aient obtenu l'identité du jeune à partir de techniques de reportage ordinaires, plutôt que de source officielle, n'était pas déterminant, a écrit le juge Burger. Il a en outre conclu que l'intérêt de l'État à protéger le mineur n'était pas suffisant pour justifier une sanction pénale, en particulier lorsque l'interdiction de la Loi ne s'appliquait pas aux médias électroniques, mais était plutôt limitée aux « journaux ». Le Juge Burger a également remis en question la nécessité d'une sanction pénale dans cette situation, notant que bien que chaque État ait une loi prévoyant un certain type de confidentialité pour les délinquants juvéniles. Seuls cinq ont imposé des sanctions pénales aux non-parties pour la divulgation de leurs noms²⁹⁹.

La Cour conclut donc que les droits protégés par le premier amendement de la Constitution des défenseurs (la presse) prévalent sur l'intérêt à protéger les mineurs. Même en supposant que la Loi servait un intérêt de l'État d'ordre public, la Loi n'accomplit pas son objectif déclaré, puisqu'elle ne restreint pas les médias électroniques ou toute forme de publication à l'exception des journaux³⁰⁰.

2.1.5 L'affaire *Florida Star c. B.J.F*

Une décennie plus tard, la Cour suprême des États-Unis a encore une fois eu l'occasion d'endurcir leur position relativement à la primauté de la presse du premier amendement de la Constitution sur la législation des États qui tente de protéger la vie privée. Dans l'affaire *Florida Star c. B.J.F* de 1989³⁰¹, la Cour suprême a statué que le premier amendement empêchait un journal d'être tenu civilement responsable en vertu du droit de la responsabilité délictuelle de l'État pour avoir publié le nom d'une victime d'agression

²⁹⁹ *Smith c. Daily Mail Publishing Co*, *supra* note 297.

³⁰⁰ *Ibid.* Voir aussi: 1^o St. Draft, Supreme Court of the United States, no 78-482, Robert K. Smith, Ect., et Al. V. Daily Mail Publishing Co. Etc., et d. May 18, 1979. Ce document contient les notes manuscrites du juge en Chef de la Cour. Disponible en ligne (21 juillet 2022) : <<https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1422&context=casefiles>>

³⁰¹ *Florida Star c. B.J.F.* (1989) 419 U.S. 524.

sexuelle. La décision rappelle celle rendue dans l'arrêt *Cox Broadcasting Corp. C. Cohn* (1975) déjà discuté.

On peut résumer les faits de cette cause ainsi : le Florida Star a publié le nom complet d'une victime de vol et d'agression sexuelle dans la section de faits divers « Police Report » de son journal édition du 24 octobre 1983. Ce faisant, le journal a violé à la fois sa propre politique interne et une loi de la Floride interdisant la diffusion de l'identité d'une victime d'agression sexuelle « dans tout instrument de communication de masse », ce qui inclut naturellement les journaux BJE est la victime dans cette affaire dont l'identité a été diffusée, a intenté une demande en justice devant le tribunal de la Floride, alléguant notamment que le Star avait porté atteinte à sa vie privée par négligence. Le tribunal de première instance a rejeté la requête en irrecevabilité du Star, qui affirmait, entre autres, que l'imposition de sanctions civiles au journal conformément à la Loi floridienne violait le premier amendement de la constitution. Cependant, il a accueilli la requête de la victime BJE pour un verdict dirigé sur la question de la négligence.

La Cour conclut que le Star a commis une faute par sa négligence d'avoir diffusé le nom de ladite victime sur la base de la Loi de l'État de la Floride l'interdisant. Le jury a alors accordé à BJE des dommages-intérêts compensatoires et punitifs. Le verdict fut confirmé puisque la Cour d'appel de la Floride a refusé l'examen du dossier³⁰². La Cour suprême des États-Unis a annulé la décision de première instance par une majorité de six contre trois juges. La Cour suprême affirme que d'imposer des dommages-intérêts au Star pour avoir publié le nom de la victime viole l'article premier amendement de la constitution³⁰³.

Contrainte par le premier amendement et leur propre jurisprudence, la Cour reconnaît et explique :

La sensibilité et l'importance des intérêts présentés dans les conflits entre le premier amendement et le droit à la vie privée conseillent à la Cour de s'appuyer sur des principes limités qui ne vont pas plus loin que le contexte approprié de l'espèce, plutôt que d'accepter des invitations à affirmer largement que la publication véridique ne peut jamais être punie

³⁰² *Ibid* aux pp 526-528.

³⁰³ *Ibid* aux pp 536-537.

conformément au premier amendement ou que la publication du nom d'une victime de viol ne bénéficie jamais d'une protection constitutionnelle. L'un de ces principes est que si un journal obtient légalement des informations véridiques sur une question d'importance publique, les responsables de l'État ne peuvent pas sanctionner constitutionnellement la publication d'information en l'absence d'un besoin de promouvoir un intérêt de l'État qui doit être de la plus haute importance « highest order » en faisant référence à l'arrêt *Smith c. Daily Mail Publishing Co*³⁰⁴.

En appliquant ce principe, la Cour a estimé que le journal Florida Star avait obtenu le nom de la victime BJJ à partir d'un rapport de police dans la salle de presse du bureau du Shérif, l'information véridique sur un événement digne d'intérêt public avait été obtenue légalement³⁰⁵.

Finalement, la Cour n'a pas considéré la protection de l'identité d'une victime d'agression sexuelle comme intérêt de l'État de première importance « highest Order », et elle conclut que la Loi de l'État de la Floride, que le journal avait enfreint, était peu inclusive, car elle punissait les instruments de communications de masse (masse média), mais aucune autre entité ou personne pour la diffusion de l'identité d'une victime de viol. La Cour suprême a également remis en question l'équité procédurale de la norme de responsabilité stricte de la Loi de la Floride sur la question de la divulgation de l'identité d'une victime et à exprimer sa crainte que la confirmation du jugement de première instance n'engendre dans le futur l'autocensure des médias. C'est ainsi que la Cour infirme le jugement de l'État de la Floride³⁰⁶.

Cette jurisprudence constante illustre parfaitement la situation aux États-Unis. Malgré le droit des États d'établir de lois d'exception visant la protection de certaines catégories d'informations à caractère personnel, incluant les informations dites sensibles, le premier amendement de la constitution américaine aura préséance si les informations ont été reçues en toute légalité, excepté dans le cas d'une démonstration par le demandeur d'un intérêt de

³⁰⁴ *Ibid* aux pp 540-541

³⁰⁵ *Ibid* aux pp 542-543.

³⁰⁶ *Ibid in fine*.

la plus haute importance³⁰⁷. Toutefois, aucune décision n'a jusqu'à maintenant réussi à atteindre ce critère exigé par la Cour suprême américaine³⁰⁸. On constate explicitement la limite qu'a le droit au respect de la vie privée pour les Américains, balayés par les vents dominants de la liberté d'expression et de presse. À ce stade de notre étude du sujet, nous pouvons observer que l'inaction des États-Unis face aux droits de la protection de la vie privée et à la protection des personnes physiques à l'égard du traitement des informations personnelles nous apparaît être contraire à la réalité actuelle, compte tenu de la trajectoire évolutive de la technologie, aux réseaux numériques, l'Internet en particulier et la capacité de rétention des données quasi infinie³⁰⁹. C'est peut-être de l'ignorance volontaire ou l'acceptation de la capacité des acteurs privés du monde numérique de s'autoréguler, mais pour le moment nous n'avons pas la réponse à cette énigme³¹⁰.

2.1.6 Projet de Loi le Data Care Act.

Notons toutefois un dépôt d'un projet de loi du Data Care Act., une première réglementation fédérale en matière de protection des données aux États-Unis.

Selon un communiqué de presse du 23 mars 2021 du bureau sénatorial, le sénateur américain Brian Schatz (Démocrate d'Hawaï) a dirigé un groupe de 17 sénateurs pour réintroduire une législation visant à protéger les données personnelles des personnes en ligne. La Loi sur la protection des données obligerait les sites Web, les applications et les

³⁰⁷ Jasmine E. McNealy, "The Emerging Conflict between Newsworthiness and the Right to be Forgotten", (2012) 39: 2 N.K.L.R. 119.

³⁰⁸ Robert Kirk Walker, "The right to be Forgotten", (2012) 64 :101 H.L. j 274.

³⁰⁹ Viktor and Mayer-Schoenberger, *supra* note 13 aux pp 15-16.

³¹⁰ Voir l'article de Consumer Watch dog sur leur site, en date du 7 juillet 2015 sur le sujet : « *Google's Failure To Offer 'Right to Be Forgotten' In United States is Unfair And Deceptive, Consumer Watchdog Tells Federal Trade Commission in Complaint* » (*L'échec de Google d'offrir un « droit à l'oubli » aux États-Unis est déloyal et trompeur, dit le Consumer Watchdog à la Federal Trade Commission dans sa plainte*) (7 juillet 2015) en ligne : <<https://www.prnewswire.com/news-releases/googles-failure-to-offer-right-to-be-forgotten-in-united-states-is-unfair-and-deceptive-consumer-watchdog-tells-federal-trade-commission-in-complaint-300109265.html>> (consulté le 15 août 2022).

autres fournisseurs en ligne à prendre des mesures responsables pour protéger les informations personnelles et mettre fin à l'utilisation abusive des données des utilisateurs.

Le sénateur Schatz a déclaré :

[I]es sites Web et les applications qui collectent des informations personnelles ont la responsabilité de protéger ces données et de ne pas les utiliser d'une manière qui nuit à leurs propres utilisateurs. Notre projet de loi aidera à s'assurer que lorsque les gens donnent leurs renseignements aux entreprises en ligne, ils ne seront pas abusés³¹¹.

Ce dernier déclare et compare que si les médecins, les avocats et les banquiers sont légalement tenus d'exercer une attention particulière pour protéger leurs clients et de ne pas abuser de leurs informations. Bien que les entreprises en ligne détiennent également des informations personnelles et sensibles sur les personnes qu'elles servent, elles ne sont pas tenues de protéger les données des consommateurs. Cela laisse les utilisateurs dans une position vulnérable. On s'attend à ce qu'ils comprennent les informations qu'ils donnent aux fournisseurs et comment elles sont utilisées. En établissant une obligation explicite pour les fournisseurs en ligne, les Américains peuvent être sûrs que leurs données en ligne sont protégées et utilisées de manière responsable.

La Loi sur la protection des données établit des obligations raisonnables qui obligeront les fournisseurs à protéger les données des utilisateurs et interdiront aux fournisseurs d'utiliser les données des utilisateurs à leur détriment :

Devoir de diligence : Doit sécuriser raisonnablement les données d'identification individuelles et informer rapidement les utilisateurs des violations de données impliquant des informations sensibles ;

Devoir de loyauté : Ne peut pas utiliser les données d'identification individuelles de manière à nuire aux utilisateurs ;

³¹¹ Brian Schatz, "Schatz Leads Group Of 17 Senators In Reintroducing Legislation To Help Protect People's Personal Data Online" (23-03-2021) en ligne: <<https://www.schatz.senate.gov/news/press-releases/schatz-leads-group-of-17-senators-in-reintroducing-legislation-to-help-protect-peoples-personal-data-online>>

Devoir de confidentialité : Doit s'assurer que les devoirs de diligence et de loyauté s'étendent aux tiers lors de la divulgation, de la vente ou du partage de données d'identification individuelles ;

Application fédérale et étatique : Une violation des devoirs sera traitée comme une violation d'une règle de la FTC avec une amende. Les États peuvent également engager des poursuites civiles, mais la FTC peut intervenir. Les États et la FTC peuvent poursuivre les collecteurs de données propriétaires et tiers ;

Autorité de réglementation : La FTC se voit accorder l'autorité de réglementation pour mettre en œuvre la Loi³¹².

Il s'avère que contrairement à l'Union européenne, le projet de Loi Data Care Act ne fait pas de place à un droit à l'oubli numérique.

En conclusion, il ne s'agit pas de la première tentative de faire passer une loi fédérale, d'application générale devant la chambre législative américaine³¹³. Cependant, depuis l'adoption du Règlement général sur la protection des données (RGPD), nous semblons être à un point tournant en matière de réglementation sur la protection des données numériques dans plusieurs pays. Il sera donc intéressant de suivre le développement de ce projet de loi et ses amendements, mais aussi le désir des Américains à ce qu'il devienne une véritable loi.

³¹² Titres officiels tels qu'introduits: S. 919: Data Care Act of 2021, du 23 mars 2021, 117 th. Congress/ St. Session, en ligne: <https://www.congress.gov/bills/117/senate/919/all-infoov/bill/117th-congress/senate-b>.

³¹³ Éloïse Gratton, « Une nouvelle loi en matière de protection de renseignements personnels aux États-Unis? », (7 février 2015), en ligne : <<https://www.eloïsegratton.com/blog/2015/02/07/une-nouvelle-loi-en-matiere-de-protection-de-renseignements-personnels-aux-etats-unis/>> (consulté le 15 août 2022).

2.2 L'ÉVOLUTION AU CANADA

En 2016, le Commissariat à la protection de la vie privée du Canada a mené des consultations pour savoir comment le droit à l'oubli s'appliquerait dans le contexte canadien³¹⁴.

En 2018, le Commissariat à la protection de la vie privée a publié un projet de position de principe sur la réputation en ligne, englobant le droit à l'oubli, à la suite de cette consultation³¹⁵. À la lumière des mémoires reçus et de sa propre analyse, il préconise des solutions permettant de trouver un équilibre en la liberté d'expression et les intérêts des personnes en matière de protection.

Selon le commissariat, il ressort de la consultation que la population canadienne « est de plus en plus préoccupée par leur réputation en ligne et déplore l'absence de mécanismes de contrôle pour se protéger contre les risques d'atteinte à leur réputation en ligne³¹⁶ ».

Le Commissariat constate que les Canadiens ont besoin de meilleurs outils pour les aider à protéger leur réputation en ligne. Ainsi, le projet de position met en évidence les mesures de protection prévues par la Loi fédérale sur la protection des renseignements personnels dans le secteur privé au Canada, désigne des changements législatifs éventuels et propose d'autres solutions pertinentes. Ces solutions comprennent le droit de demander aux opérateurs de moteurs de recherche le déréférencement de pages Internet qui renferme des

³¹⁴ Commissariat à la protection de la vie privée du Canada, Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques, mai 2016, en ligne: https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat-recherche-consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2016/consent_201605/. Le Commissariat à la protection de la vie privée au Canada offre des conseils et de l'information aux personnes sur la façon de protéger leurs renseignements personnels. Le Commissariat est également chargé de l'application des deux lois fédérales sur la protection de la vie privée : Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Loi sur la protection des renseignements personnels.

³¹⁵ Commissariat à la protection de la vie privée du Canada : selon le commissaire à la protection de la vie privée, des améliorations s'imposent pour protéger la réputation, (26 janvier 2018) en ligne : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2018/nr-_180126/

³¹⁶ *Ibid.*

renseignements inexacts, incomplets ou obsolètes, l'effacement et/ou la modification de l'information à la source³¹⁷.

Le rapport, qui fait état de ces deux mécanismes du droit à l'oubli, découle de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)³¹⁸ qui a pour but d'améliorer le contrôle exercé par les personnes sur leur réputation sur Internet.

Outre, le référencement, l'effacement à la source, le rapport présente plusieurs mécanismes et propositions visant à améliorer le contrôle par les personnes sur leurs données à caractère personnel sur Internet³¹⁹.

Voici les propositions énoncées dans le projet de position du Commissariat : « Le parlement devrait envisager d'enchâsser dans la loi quasi absolue des jeunes d'obtenir l'effacement de renseignements qu'ils ont eux-mêmes affichés en ligne ou fournis à une organisation afin qu'elle les affiche. Le Parlement devrait envisager de permettre aux jeunes, lorsqu'ils atteignent l'âge de la majorité, de demander et d'obtenir l'effacement de renseignements à leur sujet affichés en ligne par leurs parents ou tuteurs. Le Commissariat s'est engagé à prendre des mesures proactives pour régler les problèmes systémiques ou sectoriels touchant la réputation en ligne, par exemple lorsqu'il s'agit de groupes vulnérables. Le Commissariat s'est aussi engagé à encourager la recherche portant sur de nouvelles solutions en matière de protection des renseignements en ligne ainsi que l'élaboration et l'adoption de ces solutions, notamment dans le cadre de son Programme des contributions. Il faudrait élaborer un code de pratique à l'échelle de l'industrie concernant les politiques d'effacement des renseignements, les paramètres par défaut et les procédures de protection de la vie privée »³²⁰.

³¹⁷ *Ibid.*

³¹⁸ Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000 C-5.

³¹⁹ Commissariat à la protection de la vie privée du Canada, *supra* note 315 à la p 3.

³²⁰ *Ibid* à la p 4.

L'objectif canadien est de créer un environnement sur Internet où les personnes peuvent se servir des outils numériques sans craindre que leur trace numérique n'entraîne un traitement arbitraire et injuste. Le Commissariat à la protection de la vie privée du Canada a fait de réputation et la protection de la vie privée l'une de ses priorités stratégiques liées à la réalité numérique d'aujourd'hui³²¹. L'étude à laquelle s'est engagé le Commissariat au sujet de la réputation en ligne a de quoi rappeler l'introduction du droit à l'oubli ou droit à l'effacement, prévu par le Règlement général sur la protection des données RGPD de l'Union européenne. À la suite de l'examen sur la question, le Commissariat est préoccupé par l'absence de mécanismes de contrôle sur le traitement des données à caractères personnels d'une part et la liberté d'expression invoquée par l'industrie numérique d'autre part³²².

2.2.1 Liberté d'expression et l'équilibre avec la protection de la vie privée

Au Canada aussi, l'interaction qui existe entre la protection de la vie privée et d'autres valeurs, comme la liberté d'expression a présenté un intérêt marqué pour le Commissariat dans l'évaluation des mécanismes de contrôle de la réputation numérique de la personne. En effet, les défenseurs de la vie privée argumentent que les personnes devraient pouvoir exercer un contrôle sur la présence ou l'accessibilité de leurs renseignements personnels, mais dans certains cas, il va de l'intérêt de la collectivité à s'assurer que ces informations demeurent publiques. Il est donc nécessaire de mettre en balance la vie privée des personnes et la liberté d'expression³²³.

³²¹ *Ibid* à la p 5.

³²² *Ibid* à la p 5.

³²³ *Ibid*.

2.2.2 Considération des principes à valeur constitutionnelle canadienne

2.2.3 Irwin Toy Ltd c. Procureur général du Québec

Au Canada, la liberté d'expression est protégée par l'article 2 b) de la Charte canadienne des droits et libertés³²⁴ qui est définie par la Cour suprême du Canada dans l'arrêt Irwin Toy Ltd³²⁵ signifiant « La garantie que nous pouvons communiquer nos pensées et nos sentiments de façon non violente, sans crainte de censure »³²⁶. La liberté d'expression doit recevoir une interprétation d'une vision de l'engagement démocratique³²⁷. Dans cette affaire, il s'agissait de déterminer si la publicité destinée aux enfants entre dans le champ de liberté d'expression ? La Cour répond qu'elle a déjà affirmé à plusieurs reprises que les droits et libertés garantis par la Charte canadienne doivent recevoir une interprétation large et libérale et, par conséquent, il n'a aucune raison valable d'exclure l'expression commerciale de la protection de l'article 2 b) de la Charte³²⁸. La Cour suprême du Canada a assidûment soutenu que le concept de liberté d'expression doit recevoir une « interprétation large et libérale » ce qui a été répété dans l'arrêt Ford³²⁹ un an auparavant.

Selon la Cour suprême, l'article 2b) de la Charte canadienne doit être analysé en fonction d'un critère à trois volets : l'activité en question a-t-elle le contenu expressif nécessaire pour entrer dans la sphère d'application de la protection offerte par l'alinéa 2 b) ? Le lieu où le mode d'expression ont-ils pour effet d'écarter cette protection ? Si l'activité expressive est protégée par l'alinéa 2b), est-ce que la mesure gouvernementale, du fait de

³²⁴ Charte canadienne des droits et libertés, art 2 b, partie I, de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R.U.), 1982, c 11,

³²⁵ Irwin Toy Ltd c. Québec (Procureur général), 1989 1 RCS 927.

³²⁶ *Ibid* à la p 969.

³²⁷ *Ibid* à la p 970.

³²⁸ *Ibid* à la p 971.

³²⁹ Ford c. Québec (Procureur général) 1988 2 RCS 712, au para 59.

son objet ou son effet, porte atteinte au droit protégé ? *Société Radio-Canada c. Canada*³³⁰, *Ville de Montréal c. 2952-1366 Québec Inc.*³³¹, et *Irwin Toy Ltd.* Précité.

La liberté d'expression comprend plus que le droit d'exprimer des croyances et des opinions ; elle protège tout autant celui qui s'exprime que celui qui l'écoute (*Edmonton Journal c. Alberta*) (Procureur général)³³². Par « expression » s'entendent également toutes les étapes de la communication, depuis le concepteur ou l'expéditeur jusqu'au destinataire, qu'il s'agisse d'un auditeur ou spectateur, en passant par le fournisseur, le distributeur, le détaillant, le locateur et l'exposant *Dagenais c. Société Radio-Canada*³³³ ; *Irwin Toy Ltd.*, précité ; *Rocket c. Collège royal des chirurgiens-dentistes de l'Ontario*³³⁴ ; *R. c. Videoflicks*³³⁵.

2.2.4 L'action gouvernementale et la liberté d'expression

Si l'objet de l'action gouvernementale consiste à restreindre le contenu de l'expression, à contrôler l'accès à un certain message ou à limiter la possibilité pour une personne de transmettre un message afin de s'exprimer, cet objet sera contraire à l'alinéa 2b) *Irwin Toy Ltd.*, précité³³⁶.

Même si l'objet est compatible avec l'alinéa 2b) de la Charte canadienne, une personne pourra établir que la restriction gouvernementale a comme effet de porter atteinte à son droit garanti par l'alinéa 2 b). Cette personne devra faire la preuve qu'une expression vise les fins de l'alinéa 2 b), c'est-à-dire la participation à la prise de décisions d'intérêt social

³³⁰ *Société Radio-Canada c. Canada* (Procureur général) 2011 1 RCS 19.

³³¹ *Montréal (Ville) c. 2952-1366 Québec Inc.* 2005 3 RCS 141.

³³² *Edmonton Journal c. Alberta* (Procureur général) 1989 2 RCS 1326.

³³³ *Dagenais c. Société Radio-Canada*, 1994 3 RCS 835.

³³⁴ *Rocket c. Collège Royal des chirurgiens-dentistes de l'Ontario*, 1990 2 RCS 232.

³³⁵ *R. c. Videoflick*, 1984, 14 D.L.R. (4th) 10.

³³⁶ *Irwin Toy Ltd c. Québec* (Procureur général), *supra* note 325 à la p 976.

et politique, la recherche de la vérité ainsi que l'épanouissement personnel, Irwin Toy, précitée³³⁷.

Si un tribunal détermine que l'objet ou l'effet de l'action gouvernementale porte atteinte au droit garanti par l'alinéa 2 b), il examinera ensuite si cette restriction peut être justifiée au regard de l'article premier de la Charte canadienne³³⁸.

2.2.5 Liberté d'expression n'est pas absolue

2.2.6 Aubry c. Éditions Vice-Versa Inc.

La Cour suprême a également indiqué que si grande que soit la liberté d'expression, elle n'est pas absolue, ainsi dans l'affaire *Aubry c. Éditions Vice-Versa Inc.* De 1998³³⁹ reposant sur les faits suivants, l'intimé a intenté une demande en responsabilité civile contre les appelants *Éditions Vice-Versa Inc.* Et un photographe, pour avoir pris et publié dans une revue à vocation artistique une photographie d'une jeune fille, alors âgée de 17 ans, assise sur les marches d'un édifice dans un lieu public. La photographie a été publiée sans le consentement de la jeune fille intimée³⁴⁰.

Le juge de première instance a reconnu que la publication sans autorisation de la photographie constituait une faute et a condamné solidairement l'Éditeur et le photographe à payer la somme de 2 000 \$ en dommages. La Cour d'appel, à la majorité, a confirmé cette décision. La Cour suprême du Canada affirme ce qui suit :

En l'espèce, la responsabilité des appelants est à priori engagée puisqu'il y a eu publication de la photographie alors que l'intimée était identifiable. Nous ne croyons pas que l'expression artistique de la photographie, dont on a allégué qu'elle servait à illustrer la vie urbaine

³³⁷ *Ibid* à la p 977.

³³⁸ Charte canadienne article 1 : « La Charte canadienne des droits et libertés garantit les droits et libertés qui y sont énoncés. Ils ne peuvent être restreints que par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique ».

Charte canadienne des droits et libertés, *supra* note 324.

³³⁹ *Aubry c. Édition Vice-Versa Inc.*, 1998 1 RCS 591.

³⁴⁰ *Ibid.*

contemporaine, puisse justifier l'atteinte au droit à la vie privée qu'elle comporte. L'argument que le public a intérêt à prendre connaissance de toute œuvre artistique ne peut être retenue, notamment parce que le droit de l'artiste de faire connaître son œuvre, pas plus que les autres formes de liberté d'expression, n'est absolu. Il y a en effet lieu de rappeler ici le texte de l'art. 9.1 de la Charte québécoise de même que le fait que notre Cour a affirmé à plusieurs reprises que la liberté d'expression doit être délimitée en tenant compte des autres valeurs en présence. Voir *Fraser c. Commission des relations de travail dans la Fonction publique*, [1985] 2 R.C.S. 455 ; *Dagenais c. Société Radio-Canada*, [1994] 3 R.C.S. 835, et *Hill c. Église de scientologie de Toronto*, [1995] 2 R.C.S. 1130, au para. 103 Voir aussi *Moises c. Canadian Newspaper Co.*, [1997] 1 W.W.R. 337 (C.A.C.-B.)³⁴¹.

Tout comme les États membres de l'Union européenne, le défi consiste donc à envisager des dispositions législatives assurant un juste équilibre entre, la vie privée des personnes et les valeurs tout aussi importantes protégées par la liberté d'expression.

2.2.7 Hill c. Église de scientologie

Dans la décision *Hill c. Église de scientologie*,³⁴² la Cour suprême a déterminé trois principes qui sont à la base de la liberté d'expression, soit l'épanouissement individuel, la recherche de la vérité et la promotion du discours démocratique. Elle mentionne qu'il est possible que les personnes dont la réputation est indûment ternie ne soient pas en mesure de participer entièrement au discours public. Dans certaines circonstances, il se peut qu'on les ignore, qu'ils perdent de la crédibilité, plus encore que leur contribution propice à l'émergence de nouvelles idées soit préjugée en fonction de leur réputation plutôt que son contenu. À ce sujet la Cour déclare :

En outre, la réputation est étroitement liée au droit à la vie privée, qui jouit d'une protection constitutionnelle. Comme le juge Laforest le dit dans *R. c. Dymont (1988) 2 RCS 417*, à la page 427, « la vie privée y compris la vie privée sur le plan informationnel est fondée sur l'autonomie morale et physique de la personne et essentielle à son bien-être. La publication de commentaires diffamatoires constitue une intrusion dans la vie privée d'un individu et un affront à sa dignité. La réputation d'une personne mérite effectivement d'être protégée dans notre société démocratique et cette protection doit être soigneusement mesurée en regard du droit tout aussi important à la liberté d'expression³⁴³.

³⁴¹ *Ibid* au para 62.

³⁴² *Hill c. Église de scientologie de Toronto*, 1995 2 RC 1130.

³⁴³ *Ibid* au para 121.

2.2.8 Grant c. Torstar Corp.

Dans le même ordre d'idée, dans *Grant c. Torstar Corp*, la Cour suprême conclut, sans équivoque :

Des trois raisons d'être de la protection constitutionnelle de la liberté d'expression, seule la troisième, l'épanouissement personnel, a plus ou moins de pertinence en matière de communication diffamatoire concernant une question d'intérêt public. Cela tient à ce que la réputation du demandeur peut mériter d'être tout autant que l'épanouissement personnel passant par l'expression exempte d'entraves. Il n'est pas question ici d'une *interdiction* de s'exprimer décrétée par l'État, où même l'épanouissement personnel par l'expression malveillante ou trompeuse peut entrer en ligne de compte (*R. c. Zundel*, [1992] 2 R.C. S. 731), mais d'un moyen par lequel une personne peut en rechercher une autre en responsabilité civile en raison des propos que cette dernière a tenus. Les principes de la Charte n'autorisent personne à ternir la réputation d'autrui pour le simple assouvissement du désir atavique de s'exprimer³⁴⁴.

Bien que les deux déclarations ci-haut mentionnées figurent dans des décisions portant sur des affaires en matière de diffamation, on peut faire valoir l'argument que la Cour suprême du Canada va sûrement appliquer les mêmes principes qui protègent la réputation de façon plus générale, notamment en vertu des lois sur la vie privée au Canada. Compte tenu de ce qui précède, la Cour suprême semble avoir atteint cet équilibre de respect à la fois la liberté d'expression et les intérêts en matière de vie privée.

2.2.9 Loi sur la protection des renseignements personnels et des documents électroniques

À la suite de cette analyse, le Commissariat à la protection de la vie privée au Canada et après examen de la jurisprudence en la matière mentionnée, a déclaré que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) s'applique aux entreprises ayant des activités commerciales au Canada, conséquemment confère aux Canadiennes et Canadiens le droit de contester l'exactitude et l'intégralité de leurs renseignements personnels et d'exiger des entreprises qui recueillent ces

³⁴⁴ *Grant c. Toronto Corp*, 2009 3 RCS 640, au para 51.

renseignements qu'elles les modifient ou les suppriment s'ils s'avèrent inexacts, incomplets ou obsolètes³⁴⁵.

2.2.10 Renvoi à la Cour fédérale 2021 CF 723

Pour s'en assurer, le commissaire a renvoyé la question de la nature commerciale des acteurs proposant des moteurs de recherches à la Cour fédérale³⁴⁶, dans le présent renvoi présenté en marge de l'enquête du commissaire sur une plainte déposée en juin 2017 contre Google LLC, sur une demande de déréférencement. En date du 8 juillet 2021, la juge en chef adjointe Jocelyne Gagné, dans le cadre du renvoi (2021 FC 723, 8 juillet 2021)³⁴⁷ doit répondre à deux questions concernant l'application de LPRPDE à ce moteur de recherche spécifiquement : est-ce que Google, dans le contexte de son service de moteur de recherche, recueille, utilise ou divulgue des renseignements personnels dans le cadre d'activités commerciales au sens de l'alinéa 4(1)a) de la LPRPDE lorsqu'elle indexe des pages Web et présente des résultats de recherche en réponse à des recherches quant au nom d'un individu ?

L'exploitation du service de moteur de recherche de Google est-elle exclue de l'application de la partie 1 de la LPRPDE en vertu de l'alinéa 4(2)c) de la LPRPDE parce qu'elle implique la collecte, l'utilisation ou la divulgation de renseignements personnels à des fins journalistiques, artistiques ou littéraires et pour aucun autre but ?

La Cour fédérale répond à la première question par l'affirmative et explique pourquoi :

³⁴⁵ Commissariat à la protection de la vie privée du Canada, Communiqué du 26 janvier 2018 : selon le commissaire à la protection de la vie privée, des améliorations d'imposent pour protéger la réputation en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2018/nr-c_180126/> (consulté le 16 août 2022). Voir aussi : Commissariat à la protection de la vie privée du Canada, Rapport de conclusions en vertu de la LPRPDE no. 2019-002, 25 avril 2019.

³⁴⁶ Le commissaire à la protection de la vie privée du Canada a soumis un renvoi en vertu du paragraphe 18.3 (1) de la Loi sur la Cour fédérale, LRC 1985, CF-7, qui permet aux offices fédéraux de renvoyer à la Cour, à n'importe quelle étape de ses procédures, toute question de droit, de compétence ou de pratique et procédure.

³⁴⁷ Renvoi relatif au titre du paragraphe 18.3 (1) de la Loi sur les Cours fédérales, 2021 Cf 723.

[40] Les sous-questions pertinentes pour cette première question sont de savoir si a) dans le contexte du fonctionnement du service de moteur de recherche de Google, lorsqu'elle indexe des pages Web et présente des résultats de recherche en réponse à des recherches portant sur le nom d'un individu, Google divulgue, collecte ou utilise des renseignements personnels, et b) si elle le fait dans le cadre d'activités commerciales.

[51] Google est une société à but lucratif et l'une des entreprises technologiques les plus prospères de l'ère moderne.

[52] La majeure partie des revenus de Google provient de la publicité.

[53] Les annonceurs paient à Google des frais chaque fois qu'un utilisateur clique sur une annonce dans les résultats de recherche Google ou effectue une action après avoir vu une annonce, comme le téléchargement d'une application.

[54] Étant donné que Google diffuse également des annonces sur des sites Web tiers, Google peut générer des revenus si un utilisateur accède à une page Web répertoriée dans les résultats de recherche Google, puis clique sur ou consulte une annonce fournie par Google affichée sur cette page.

[55] Google fait la promotion de ses activités publicitaires en mettant de l'avant la popularité de son moteur de recherche.

[56] Ce modèle d'affaires était anticipé lorsque le Parlement a adopté la LPRPDE. Le document de consultation du gouvernement du Canada qui a précédé la LPRPDE notait que le défi de l'ère électronique est qu'avec chaque transaction, nous laissons une trace de données qui peuvent être compilées pour fournir un dossier détaillé de notre histoire personnelle et de nos préférences (pièce D-1 de l'affidavit Ballott p. 23). Dans ce nouvel environnement, les renseignements personnels eux-mêmes deviennent une marchandise, à extraire et à utiliser à des fins lucratives (pièce D-1 de l'affidavit Ballott p. 23).

[57] C'est-à-dire que même si Google fournit des services gratuits aux fournisseurs de contenu et à l'utilisateur du moteur de recherche, elle a un intérêt commercial flagrant à connecter ces deux acteurs. Il existe un véritable échange entre Google et les utilisateurs de son moteur de recherche. En échange des informations affichées dans les résultats de recherche, les utilisateurs fournissent divers renseignements personnels (leur localisation, leurs préférences, leurs intérêts, leurs habitudes de consommation, etc.). Ces renseignements personnels sont utilisés à des fins lucratives.

[58] Et, afin d'attirer les utilisateurs, Google doit leur fournir les informations les plus précises et les plus personnalisées qu'ils recherchent.

[59] Par conséquent, à moins d'y être contraint, Google n'a aucun intérêt commercial à désindexer ou à retirer des informations de son moteur de recherche. À mon avis, chaque élément de ce modèle d'affaires est une activité commerciale au sens de la LPRPDE. Porter un regard microscopique sur l'aspect gratuit (c'est-à-dire, aucun paiement en argent) de la recherche de l'utilisateur, ou sur l'aspect gratuit du service de bibliothèque fourni aux médias serait, à mon humble avis, mal comprendre le modèle économique de Google. Toutes ces activités sont étroitement liées, elles dépendent les unes des autres et elles sont toutes des composantes nécessaires de ce modèle d'affaires.

La Cour fédérale répond à la négative à la deuxième question pour les raisons suivantes :

[81] J'accepte que Google facilite l'accès à l'information, au même titre que les médias. Je conviens également que faciliter l'accès à l'information est souvent associé à la « publication » de ladite information.

[82] À mon avis, les raisons pour lesquelles les hyperliens ne sont pas considérés comme des publications à des fins de diffamation sont également pertinentes pour les résultats de recherche – Google n’a aucun contrôle sur le contenu des résultats de recherche, les résultats de recherche eux-mêmes n’expriment aucune opinion et Google ne crée pas le contenu des résultats de recherche.

[86] À mon avis, le fonctionnement du moteur de recherche de Google, même lorsqu’on ne considère que les résultats de recherche pour le nom du requérant, ne satisfait pas à la définition du journalisme acceptée par la Cour dans *Globe 24h*.

[87] L’aspect final et déterminant de cette analyse est la partie de l’alinéa 4(2)c qui précise que celui-ci ne s’applique qu’aux organisations qui recueillent, utilisent ou divulguent des renseignements personnels à des fins journalistiques, et « à aucune autre fin ».

[89] Il est utile d’appliquer une analyse similaire à Google. L’objectif principal du service de moteur de recherche de Google est d’indexer et de présenter les résultats de recherche. Il ne s’agit pas d’un objectif principalement journalistique, car bien qu’il puisse faciliter l’accès à l’information, il ne contient aucune autre caractéristique distinctive du journalisme, comme le contrôle du contenu ou la création de contenu. Même si Google fournit du journalisme dans ses résultats de recherche, ces derniers ont clairement une portée beaucoup plus large que le journalisme.

[90] En somme, le service de moteur de recherche de Google n’est pas du tout exploité à des fins journalistiques, ou du moins il n’est pas exploité à des fins exclusivement journalistiques.

[94] Et à mon avis, il n’y a pas d’ambiguïté ici. Premièrement, le Parlement a limité la LPRPDE à la seule protection du « journalisme » et non de la liberté d’expression au sens large. [...] Deuxièmement, le Parlement a limité la LPRPDE à la protection de la collecte, de la divulgation et de l’utilisation de renseignements personnels à des fins exclusivement journalistiques. Troisièmement, une compréhension populaire ou ordinaire du journalisme, telle que fournie par les journalistes eux-mêmes, n’englobe pas le service de moteur de recherche de Google.

[95] Par conséquent, je conclus que les fins de Google pour la collecte, l’utilisation et la divulgation de renseignements personnels pour son service de moteur de recherche ne sont pas journalistiques, et elles ne le sont certainement pas exclusivement³⁴⁸.

En conclusion de cette affaire importante au Canada la juge en chef adjointe Jocelyne Gagné a déclaré que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) s’applique puisque Google exerce une activité commerciale au sens de cette Loi et elle décide également que le traitement de données ou informations personnelles ne sont pas des activités journalistiques. Mme la juge Gagné rappelle que son jugement ne se veut pas une décision quant à la plainte à l’origine du renvoi judiciaire ni relativement au pouvoir du commissaire à la protection de la vie privée

³⁴⁸ *Ibid.*

(CPVP) de conseiller la désindexation, c'est-à-dire le déréférencement des liens litigieux³⁴⁹.

Le dossier sur le déréférencement est donc retourné au Commissaire (CPVP) pour décider sur la finalité de la plainte initiale à l'encontre de Google, mais aussi celle que l'exploitant du moteur pourrait s'y opposer et faire valoir autre argument³⁵⁰.

2.2.11 Loi sur la protection de renseignements personnels et des documents électroniques

Cela signifie donc que la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) s'applique et accorde déjà aux personnes du Canada le droit d'exiger son droit à l'oubli à l'encontre des opérations de moteur de recherche. Cela étant, il n'y a pas ici de vide juridique à proprement parlé³⁵¹.

En pratique, les contestations des personnes sur la pertinence ou la validité des informations la concernant, qui apparaissent au moteur de recherche, devraient être évaluées au cas par cas et les décisions quant aux déréférencements devraient tenir compte de la liberté d'expression et l'intérêt public, selon le Commissaire à la vie privée du Canada, M. Daniel Therrien³⁵².

Pour faciliter la compréhension, voici quelques dispositions de la LPRPDE à son annexe 1, principe énoncé dans la norme nationale du Canada, intitulée « Code type sur la protection des renseignements personnels »³⁵³.

³⁴⁹ *Ibid* au para 97.

³⁵⁰ *Ibid*.

³⁵¹ LC 2000 C-5, *supra* note 318 à l'article 4.1.A.

³⁵² Commissariat à la protection de la vie privée du Canada, Projet de position du Commissariat sur la réputation en ligne, 26 janvier 2018, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-la-reputation-en-ligne/pos_or_201801/> (consulté le 16 août 2022).

³⁵³ L.C. 2000, C 5, *supra* note 318. Loi à jour le 4 avril 2022.

Article 4.1 : Premier principe-responsabilité : Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

Pour les principes relatifs à l'application du droit à l'oubli et ce, même si ce droit n'est pas désigné par son nom à la présente loi.

À son article 4.6 : sixième principe-exactitude, « les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés ».

Article 4.6.1, on peut lire : Le degré d'exactitude et de mise à jour ainsi que le caractère complet des renseignements personnels dépendront de l'usage auquel ils sont destinés, compte tenu des intérêts de la personne. Les renseignements doivent être suffisamment exacts, complets et à jour pour réduire au minimum la possibilité que des renseignements inappropriés soient utilisés pour prendre une décision à son sujet.

À son article 4.5.3 : On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.

2.2.12 Le neuvième principe – Accès aux renseignements et le droit à l'oubli

L'article 4.9 stipule : Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.

Et à l'article 4.9.5 : Lorsqu'une personne démontre que des renseignements personnels sont inexacts ou incomplets, l'organisation doit apporter les modifications nécessaires à ces renseignements. Selon la nature des renseignements qui font l'objet de la contestation,

l'organisation doit corriger, supprimer ou ajouter des renseignements. S'il y a lieu, l'information modifiée doit être communiquée à des tiers ayant accès à l'information en question.

Et enfin au principe dixième, est la possibilité de porter plainte à l'égard du non-respect des principes de la présente loi.

L'article 4.10 déclare que : Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec le ou les personnes responsables de les faire respecter au sein de l'organisation concernée³⁵⁴.

À la lumière de l'analyse précédente des obligations qui incombent aux exploitants de moteur de recherche en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques, nous sommes d'avis que la Loi, actuelle au Canada, les personnes concernées seraient en mesure de pouvoir demander le déréférencement des résultats de recherche et il faudrait dans certaine circonstance faire droit à la demande.

2.2.13 Projet de loi fédérale pour protection des renseignements personnels

Le 17 novembre 2020, le gouvernement canadien a présenté le Projet de loi pour mieux protéger les données personnelles et encadrer leur utilisation par les entreprises privées. Le Projet de loi est intitulé : « Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois ».³⁵⁵ Le Projet de Loi sur la protection de la vie privée des consommateurs vise en priorité les entreprises numériques privées et l'utilisation qu'elles font des données personnelles qu'elles récoltent auprès de leurs clients sur les réseaux sociaux et sur Internet.

³⁵⁴ *Ibid.*

³⁵⁵ PLC-11, Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le tribunal de protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois, 2^e session 43^e parl, 2020. Projet de Loi C-11 (première lecture).

Ce Projet de Loi met en application les principes contenus dans la Loi sur la protection des renseignements personnels et les documents électroniques, permettra également semble-t-il, aux Canadiennes et Canadiens d'exiger que les entreprises qui détiennent leurs données à caractère personnel de les supprimer immédiatement lorsqu'ils retirent leur consentement³⁵⁶. En effet, on peut lire du projet Loi C-11 au titre de la Loi sur la protection de la vie privée des consommateurs à son article 17. (1) « l'individu peut à tout moment retirer son consentement, en tout ou en partie. Le cas échéant, il en avise l'organisation suffisamment à l'avance à 17. (2) l'organisation doit agir dès que possible à l'égard desquels le consentement a été retiré³⁵⁷. Pour assurer le respect de la loi, le gouvernement Canadien prévoit accroître les pouvoirs du Commissaire à la protection de la vie privée du Canada pour que ce dernier puisse rendre des ordonnances obligeant les entreprises à se conformer aux exigences de la loi. Dans les cas de manquement, d'importantes amendes pourraient être imposées³⁵⁸. On retrouve dans le projet de loi une certaine harmonisation avec le cadre législatif de l'Union européenne en matière de protection des données personnelles. Il reste maintenant à voir dans quelle mesure ces nouvelles protections des données personnelles canadiennes seront appliquées, advenant la promulgation de la loi.

2.2.14 La portée de la loi canadienne

Le cyberspace tend à ignorer les territoires et les frontières ; il tend à ignorer dans le même mouvement les États qu'ils bornent. Internet et ses utilisateurs sont partout et nulle part, capables d'agir en divers endroits dans le même espace-temps, et former des relations déterritorialisées. Le réseau mondial d'Internet est facilité par des moteurs de recherche dont les usagers peuvent profiter pour faire du commerce (le cybercommerce) international, mais également causer des préjudices et actes illégaux.

³⁵⁶ *Ibid.*

³⁵⁷ *Ibid* articles 17 (1) et 17 (2).

³⁵⁸ *Ibid* articles 94 (1) et (4).

2.2.15 Google Inc. C. Equustek Solutions Inc.

C'est dans cette optique que nous vous rappelons une importante décision récente de la Cour suprême du Canada, *Google Inc. C. Equustek Solutions Inc.*, de 2017³⁵⁹ dans cette affaire le plus haut tribunal du Canada a confirmé une injonction accordée dans le cadre d'un litige de propriété intellectuelle et de vol industriel à l'encontre de Google l'obligeant à déréférencer tous les sites Internet qui vendaient illégalement de produits informatiques en contravention du propriétaire légitime Equustek. La décision est unique au Canada en ce qu'elle prononce une injonction interlocutoire à portée internationale contre Google Inc. Au préalable, la Cour suprême du Canada décide que l'injonction est nécessaire et efficace pour mettre fin au préjudice subi par Equustek de la façon suivante, et nous citons :

Tout comme une ordonnance Norwich ou une injonction Mareva prononcée contre un tiers, l'injonction interlocutoire en l'espèce découle du fait que le concours de Google est nécessaire pour faciliter la violation d'ordonnances judiciaires par Datalink (fauteur du vol) et causer un préjudice irréparable à Equustek. Sans cette injonction, il était clair que Google continuerait de faciliter ce préjudice continu³⁶⁰».

En second, selon la Cour, l'octroi d'une injonction à portée internationale est le seul moyen efficace d'atténuer le préjudice subi par Equustek. Sous la plume de la juge Abella, la majorité s'exprime ainsi :

Je suis d'accord que le problème en l'espèce se pose en ligne et à l'échelle mondiale. L'Internet n'a pas de frontières – son habitat naturel est mondial. La seule façon de s'assurer que l'injonction interlocutoire atteint son objectif est de la faire appliquer là où Google exerce ses activités, c'est-à-dire mondialement. Comme l'a conclu la juge Fenlon, la majeure partie des ventes à Datalink a lieu à l'extérieur du Canada. Si l'injonction se limitait au Canada seulement ou à google.ca, ce qui aurait dû être le cas selon Google, la réparation ne pourrait pas empêcher comme il se doit le préjudice irréparable. Les acheteurs à l'extérieur du Canada pourraient facilement continuer à acheter des produits sur les sites Web de Datalink, et les acheteurs canadiens pourraient facilement trouver les sites Web de Datalink même si ceux-ci ont été délistés de google.ca. Google faciliterait toujours la violation par Datalink de l'ordonnance judiciaire lui interdisant d'exercer ses activités sur Internet. Une injonction interlocutoire n'offrant aucune possibilité d'empêcher le préjudice irréparable ne constitue pas une réparation en équité³⁶¹.

L'injonction interlocutoire en l'espèce est nécessaire pour empêcher le préjudice irréparable qui découle du fait que Datalink exploite une entreprise sur Internet, ce qu'il lui serait impossible de faire sur le plan commercial sans l'aide de Google. L'ordonnance vise les sites

³⁵⁹ *Google Inc. c. Equustek Solutions Inc.* 2017 1 RCS 824.

³⁶⁰ *Ibid* au para 35.

³⁶¹ *Google Inc. c. Equustek Solutions Inc.*, *supra* note 359 au para 41.

Web de Datalink – dont la liste a été mise à jour lorsque Datalink a voulu contrecarrer l’injonction – et interdit que ceux-ci soient affichés là où ils sont le plus dommageables, c’est-à-dire dans les résultats de recherches de Google à travers le monde³⁶².

Au nom de la majorité de la Cour du Canada, la juge Abella conclut de la façon suivante :

Google n’est pas pour autant responsable de ce préjudice. Toutefois, ces circonstances font en sorte que Google a joué un rôle déterminant en l’espèce en permettant au préjudice de se produire. Tout bien considéré, puisque l’injonction interlocutoire est la seule façon efficace de réduire le préjudice causé à Equustek jusqu’à ce que le litige sous-jacent soit réglé – la seule façon, en fait, de préserver Equustek elle-même jusqu’à ce que le litige sous-jacent soit réglé et puisque le préjudice subi par Google en contrepois est minime, voire inexistante, l’injonction interlocutoire devrait donc être confirmée³⁶³».

Et la juge Abella de rejeter le pourvoi avec dépens et de confirmer l’injonction interlocutoire mondiale à l’encontre de Google Inc.

Mécontent de la portée internationale de la décision de la Cour suprême du Canada, Google saisit la Cour fédérale de district pour le district nord de la Californie, afin d’obtenir un jugement déclarant l’injonction interlocutoire canadienne inapplicable aux États-Unis et empêcher l’exécution de ladite injonction de portée mondiale prononcée par les tribunaux canadiens et continués par la Cour suprême du Canada.

L’argument premier de Google pour invalider l’injonction est basé en partie sur les dispositions de la section 230 Communications Decency Act (47 U.S.C. 230)³⁶⁴ établit un régime de responsabilité limitée des fournisseurs de services. De plus, lors de la présentation de sa requête, Google soutenait que l’ordonnance canadienne devait être déclarée inexécutoire aux États-Unis parce qu’elle contredisait directement le droit à la liberté d’expression garantie par la Constitution américaine et qu’elle violait le principe de la courtoisie internationale. Souvenir que Google avait soulevé de semblables arguments

³⁶² *Ibid* au para 42.

³⁶³ *Ibid* au para 53.

³⁶⁴ 47 US Code s. 230 du *Communications Decency Act*.

qui ont toutefois été rejetés en ce qui concerne la liberté d'expression et la courtoisie internationale devant la Cour suprême du Canada.

En date du 2 novembre 2017, la Cour du district s'est prononcée en faveur de Google par jugement préliminaire³⁶⁵. Cette même Cour fait remarquer qu'aux termes de cette disposition, l'information litigieuse était fournie, non pas par Google en tant que moteur de recherche, mais par le distributeur contrefacteur Datalink. La Cour de district de la Californie s'explique en ces termes :

Datalink (not Google) « provides » the information at the issue. Google crawls third-party websites and adds them to its index. When a user queries Google's search engine, Google responds with links to relevant websites and short snippets of their contents. Id. Google search engine helps users discover and access content on third-party websites, but it doesn't « provide » that content within the meaning of Section 230. See O'Kroy. 831 F. 3d at 33 (holding that Google cannot be liable « for merely providing access to, and producing, the allegedly defamatory text » in the form of links and snippets in search engine results³⁶⁶).

En conséquence, le tribunal américain a fondé sa décision sur la Loi des États-Unis qui protège les fournisseurs de services informatiques et de recherche interactifs de toute responsabilité émanant de contenus créés par des tiers. La Cour fait remarquer que cette Loi aurait été adoptée pour contrer l'admonestation que les poursuites en responsabilité faisaient peser sur la soi-disant liberté d'expression sur Internet, en particulier dans les cas d'entreprises servant d'intermédiaires pour transmettre des contenus provenant de tiers.

Selon eux, en forçant les intermédiaires comme Google à supprimer les liens vers le contenu de ces tiers usagers, l'injonction canadienne va à l'encontre des objectifs et des fondements de la Loi américaine, et menace la liberté d'expression sur Internet à l'échelle planétaire. Malheureusement, cette décision de la Cour de la Californie, qui a rendu une ordonnance qui dit en faits concrets que les tribunaux canadiens n'avaient pas le droit d'ordonner à Google de délistier l'ensemble des sites Web de Datalink, en tout cas, pas aux États-Unis. Ainsi, cette décision procure une immunité certaine à Google et d'autres

³⁶⁵ *Google Inc. v Equustek Solutions Inc.*, Case no 5.17-CV-04207-EJD.

³⁶⁶ *Ibid.*

entreprises offrant le même genre de services sur le sol américain. Il convient de signaler que l'on retrouve dans cette décision américaine aucune analyse profonde ou recherche des principes de courtoisie internationale, de conflit entre les lois, de l'importance de la notion de reconnaissance des jugements étrangers, de la réalité que constituent les nouvelles technologies, et plus particulièrement Internet ou le rôle dominant que joue Google dans cette réalité mondiale.

Ce n'est pas fini ! En mars 2018, la décision de la *U.S. District Court of California North Google* demande la modification de l'ordonnance devant la Cour suprême de la Colombie-Britannique, considérant que Cour suprême du Canada avait laissé la porte ouverte à revisiter la question de la violation de la Loi d'une autre juridiction, incluant l'interférence dans la liberté d'expression³⁶⁷.

Google s'adresse donc à la Cour suprême de la Colombie-Britannique pour faire modifier l'ordonnance de délestage extraterritoriale et son exécution de ladite injonction. En avril 2018, la Cour suprême de la Colombie-Britannique, sous la plume du juge Smith, a rejeté la demande de Google en annulation ou modification de ladite ordonnance de délestage, en indiquant clairement que Google n'apportait pas de preuve que la décision canadienne portait réellement atteinte au premier amendement de la Constitution américaine ou aux principes de valeurs fondamentales du pays. De plus, la Cour fait remarquer que Google n'avait pas fait la preuve qu'un changement de circonstance militait pour une modification de l'injonction. Le juge Smith s'exprime ainsi:

I find not open to me to revisit all issues relating to extra-territoriality and judicial comity that were before all three levels of court in the prior proceedings. On those issues, the Supreme Court of Canada has defined in advance the change of circumstance that will justify a reconsideration: Google could apply to vary on the basis of evidence that the injunction would « require it to violate the laws of another jurisdiction, including interfering with freedom of expression ». Google says that should be interpreted broadly, noting that the Supreme Court of Canada cited Groberman J.A. reference to « core values ». It says the injunction violates core american values by interfering with freedom of speech³⁶⁸.

³⁶⁷ Google Inc. c. Equustek Solutions Inc., *supra* note 359 au para 46.

³⁶⁸ *Equustek Solutions Inc. c Jack* 2018 BCSC 610 (CanLII) au para 19.

Et un peu plus loin, le juge affirme :

But even if I am wrong in that, Google has not demonstrated that the injunction violates for American values. I assume rights guaranteed by the First Amendment can be regarded as core values, but Judge Davila expressly declined to rule on Google's submissions that its First Amendment rights were violated by the injunction. Google argues the First Amendment was engaged because it drives the policy underlying both the statute and the decision. In my view, the decision of Judge Davila should not be interpreted to mean more than it actually says, particularly as Google's application was unopposed and the Court did not have the benefit of any contrary arguments³⁶⁹.

Finalement, la Cour suprême de la Colombie-Britannique nous rappelle que l'indépendance de son processus décisionnel est plus importante que la perception à l'étranger de son jugement, et même si l'effet est international, préservant ainsi sa souveraineté. Et nous citons:

The effect of the U.S. order is that no action can be taken against Google to enforce the injunction in U.S. courts. That does not restrict the ability of this Court to protect the integrity of its own process through orders directed to parties over whom it has personal jurisdiction³⁷⁰.

Il semblerait qu'à la lumière de la saga Google-Equustek que les tribunaux canadiens se sont mieux adaptés dans la mise en œuvre des règles juridictionnelles évolutives pertinentes à la réalité du monde numérique et particulièrement de l'Internet. Mais on constate en même temps les difficultés de faire respecter les décisions dans ce monde virtuel sans frontière.

2.2.16 Douez c. Facebook Inc.

C'est dans cette même optique que s'inscrit une cause de 2017, *Douez c. Facebook* de la Cour suprême du Canada³⁷¹, dans cet arrêt la Cour nous rappelle la vulnérabilité des lois

³⁶⁹ *Ibid* au para 21.

³⁷⁰ *Ibid* au para 22.

³⁷¹ *Douez c. Facebook inc.* 2017 1 RCS 751.

d'ordre public et même les valeurs constitutionnelles canadiennes finiraient par être vidées de leur sens ou de leur capacité diminuée d'application dans le monde numérique d'Internet. À ce titre, nous citons quelques passages de ce jugement qui nous apparaissent comme étant des plus pertinents.

Le litige porte en l'espèce sur le droit de Mme Douez au respect de sa vie privée. Les dispositions qui garantissent ce droit se voient reconnaître un caractère quasi constitutionnel (*Lavigne c Canada [Commissariat aux langues officielles]* [1997] 2 R.C.S. 403, para. 65-66 ; *R. c Dymont* [1998] 2 R.C.S. 417, p. 427). Comme le fait observer la juge de première instance, la croissance d'Internet – un réseau quasi atemporel au rayonnement infini- a exacerbé le préjudice susceptible d'être infligé à une personne par une atteinte à son droit à la vie privée. Il est donc particulièrement important de faire en sorte que la victime d'un tel préjudice ne soit pas privée de recours. Et comme l'allégation de Mme Douez requiert l'interprétation d'un délit civil d'origine législative, seule l'interprétation par une juridiction locale des droits à la vie privée que confère la *Privacy Act* offrira aux autres résidents de la province clarté et certitude sur la portée de ces droits³⁷².

Et plus spécifiquement sur les droits constitutionnels, la Cour s'exprime ainsi :

Deuxièmement, il existe un intérêt prépondérant à ce que les tribunaux canadiens statuent dans les affaires qui portent sur des droits constitutionnels ou quasi constitutionnels, car ces droits jouent un rôle essentiel dans une société libre et démocratique et incarnent des valeurs canadiennes fondamentales. Il est foncièrement dans l'intérêt du public que les tribunaux canadiens tranchent en la matière. Par leurs décisions, les tribunaux établissent des normes et interprètent les droits dont jouissent les Canadiens³⁷³.

Comme on peut le concevoir, les difficultés sur le plan juridictionnel ne peuvent que s'aggraver avec les projets de loi canadienne qui ciblent la protection des données personnelles et son traitement considérant que la plupart des acteurs dans le monde numérique exploitant ces données sont des multinationales situées hors de la juridiction du Canada. Néanmoins, l'exemple de l'Union européenne avec leur règlement général sur la protection des données RGPD peut servir d'inspiration révocatoire pour la future bouture législative canadienne.

³⁷² *Ibid* au para 59.

³⁷³ *Ibid* au para 58.

2.3 SITUATION AU QUÉBEC

Il a quelque temps, nous vous aurions répondu que le droit à l'oubli n'existe pas au Québec, considérant une décision de la Commission d'accès à l'information du Québec du 14 avril 2016 ; *C.L. c. BCF avocats d'affaires*³⁷⁴.

2.3.1 C.L. c. BCF Avocats d'affaires

Dans cette affaire, le profil d'une employée avait été supprimé du site Internet de son ancien employeur à la suite d'une « rupture » de relation de travail, mais il subsistait toujours des résultats dans le moteur de recherche établissant un lien avec son ancien employeur. L'ex-employée était convaincue que cette situation lui causerait un préjudice dans sa recherche d'emploi, puisque les futurs employeurs effectuent nécessairement des recherches sur Internet et que cela pourrait compromettre ses chances de réussite dans sa quête d'emploi.

Après un examen du droit applicable québécois, particulièrement la Loi sur la protection des renseignements personnels dans le secteur privé³⁷⁵, la juge administrative Lina Desbiens au nom de la Commission en est venue à la conclusion que rien ne permet d'inférer l'existence d'un droit au déréférencement ou droit à l'oubli au Québec, elle souligne que :

Le droit d'une personne de faire rectifier dans un dossier qui la concerne des renseignements inexacts, incomplets ou équivoques n'est pas de l'ordre du « droit à l'oubli » qui vise à effacer des informations des espaces publics. D'ailleurs, il n'est pas certain que ce droit, bien que reconnu en Europe, trouve son application au Québec³⁷⁶.

Par conséquent la demande doit être rejetée.

³⁷⁴ C.L. c. BCF Avocats d'affaires, 2016 QCCA 114.

³⁷⁵ Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ, c.p.39.1.

³⁷⁶ *Ibid* au para 65.

Constatant l'inadéquation de la Loi existante en matière de protection des renseignements personnels, le gouvernement du Québec entreprend une transformation majeure pour mieux servir les résidents(es) du Québec face à l'évolution rapide des dernières années, des nouvelles technologies numériques utilisées dans la capture des données à caractère personnel ainsi que les esclandres récents de vol et de détournement de données personnelles au sein d'entreprises éminentes de la société québécoise.

2.3.2 Projet de Loi no 64

Or, le gouvernement du Québec a adopté le 21 septembre 2021 le Projet de Loi no 64, officiellement le titre de Loi modernisant des dispositions législatives en matière de protection des renseignements personnels³⁷⁷.

La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (PL64), a été adoptée par l'Assemblée nationale le mardi 21 septembre 2021. Il rentrera en vigueur en trois étapes à la suite de la sanction, à savoir une première partie après un an, la majorité des dispositions après trois ans³⁷⁸.

En fonction de notre présente étude, ce qui nous importe particulièrement est l'introduction du droit à l'oubli en droit québécois en vertu de cette Loi. L'analyse des dispositions de la Loi 64 nous a permis d'élucider les articles pertinents. Ainsi, à l'article 113 qui vient modifier et ajouter l'article 28.1(6) à la Loi sur la protection des renseignements personnels dans le secteur privé³⁷⁹.

Aperçu des passages pertinents de ce novateur article :

28.1. La personne par un renseignement personnel peut exiger d'une personne qui exploite une entreprise qu'elle cesse la diffusion de ce renseignement ou que soit désindexé tout

³⁷⁷ Projet de Loi no 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, en ligne : <<http://assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html>> (consulté le 16 août 2022).

³⁷⁸ Commission d'accès à l'information du Québec, « Espace évolutif-Projet de loi 64 », (21 juillet 2022) en ligne : <<https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/#>>.

³⁷⁹ Projet de Loi no 64, *supra* note 377 article 28.1.

hyperlien rattaché à son nom permettant d'accéder à ce renseignement par un moyen technologique, lorsque la diffusion de ce renseignement contrevient à la Loi ou à une ordonnance judiciaire³⁸⁰.

L'article 28.1 à son premier alinéa établit le droit aux personnes concernées de demander aux exploitants d'entreprise de cesser la transmission d'informations personnelles et de supprimer tous les liens rattachés à leur nom permettant d'accéder à cette information lorsque cette information personnelle contrevient à la Loi ou à une ordonnance judiciaire. Le deuxième alinéa précise le même droit prévu à l'alinéa 1 de l'article 28.1., mais avec la possibilité d'exiger la ré-indexation des liens attachés aux noms de la personne, lorsque les conditions suivantes réunies et qu'ils se veulent cumulatifs : 1) la diffusion de ce renseignement lui cause un préjudice grave relatif au droit au respect de sa réputation ou de sa vie privée ; 2) ce préjudice est manifestement supérieur à l'intérêt du public de connaître ce renseignement ou à l'intérêt de toute personne de s'exprimer librement ; 3) la cessation de la diffusion, la ré-indexation ou la désindexation demandée n'excède pas ce qui est nécessaire pour éviter la perpétuation du préjudice³⁸¹. Nous mentionnons les critères d'application du deuxième alinéa : 1) du fait que la personne concernée est une personnalité publique ; 2) du fait que le renseignement concerne la personnalité publique ; 3) du fait que le renseignement est à jour et exact ; 4) de la sensibilité du renseignement ; 5) du contexte dans lequel s'effectue la diffusion du renseignement ; 6) du délai écoulé entre la diffusion du renseignement et la demande faite en vertu du présent article ; 7) si le renseignement concerne une procédure criminelle ou pénale de l'obtention d'un pardon ou de l'application d'une restriction à l'accessibilité des registres des tribunaux³⁸².

Pour conclure sur la nouvelle Loi LP64, soulignons que le législateur québécois a prévu de fortes sanctions administratives en cas de violation de la loi. En effet, à l'article 90.12 prévoit un montant maximal de 50 000 \$ en cas d'une personne physique et dans les autres

³⁸⁰ *Ibid.*

³⁸¹ *Ibid* article 28.1 conditions de 1 à 3.

³⁸² *Ibid* article 28.1. 1 à 7.

cas de 10 000 000 \$ ou du montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier montant est plus élevé³⁸³.

L'article 28.1 de la Loi LP 64, n'est pas s'en rappeler l'article 17 du Règlement général sur la protection des données RGPD de l'Union européenne longuement discutée dans la présente étude, notamment sur la transposition au Québec d'un droit à l'oubli ou droit à l'effacement dans une loi miroir.

Avec l'adoption du PL64, la situation est maintenant balisée au Québec. La Loi introduit la possibilité aux personnes victimes d'atteinte à la réputation en ligne, notamment sur les moteurs de recherches et les réseaux sociaux de faire cesser ces atteintes et de demander que soit déréférencé les informations nuisibles ou devenues obsolètes, lors de toutes ordonnances ou injonctions judiciaires.

2.3.4 *In fine*

À compter du 22 septembre 2023, les personnes pourront demander aux entreprises de cesser de diffuser leurs renseignements personnels ou de désindexer tout hyperlien rattaché à leur nom donnant accès à des renseignements, si cette diffusion leur cause préjudice ou contrevient à la loi ou à une ordonnance judiciaire (droit à l'effacement ou à l'oubli)³⁸⁴.

³⁸³ *Ibid* article 90.12.

³⁸⁴ Espace évolutif-Projet de loi 64, *supra* note 378.

2.3.5 : Notions juridiques sous-jacentes au droit à l’oubli numérique : Distinction entre la protection de la vie privée et le droit à l’oubli

Il est pertinent dans le cadre de notre étude de clarifier certains concepts juridiques sous-jacents au droit à l’oubli, en supposant que leurs significations donnent aux lecteurs une meilleure compréhension de la somme de notre étude du sujet. Le droit au respect de la vie privée provient de différentes sources hiérarchisées entre elles, par exemple : la Constitution, la Charte des droits et libertés de la personne³⁸⁵, la Charte canadienne des droits et libertés³⁸⁶, ainsi que les droits étatiques comme le Code civil du Québec³⁸⁷ et les traités internationaux³⁸⁸.

Le droit à la vie privée peut être considéré comme un droit constitutionnel ou quasi constitutionnel, dépendamment des différents États. En général, ce droit se préoccupe essentiellement de la protection des informations à caractère privé d’une personne. Autrement dit, chacun de nous a le droit de s’opposer à la reproduction de son image ou de la diffusion de toute information relative à notre vie privée, de façon à ne pas être livré en pâture à l’appétence publique. Et pour sa part, le droit à l’oubli numérique est protégé de façon nominative par des lois administratives réglementant la protection des données personnelles, par exemple le (RGPD) européen de 2018 qui précise les conditions dans lesquelles une personne dispose du droit à l’oubli³⁸⁹. Selon la doctrine juridique, certains auteurs font la conciliation entre ces deux notions, expliquant que le droit à l’oubli

³⁸⁵ Charte des droits et libertés de la personne, RLRQ, 1977 C-12

³⁸⁶ Charte canadienne des droits et libertés, *supra* note 324.

³⁸⁷ Code civil du Québec, art 35 et 36 CcQ.

³⁸⁸ Le droit au respect de la vie privée figure à l’article 12 de la Déclaration universelle des droits de l’homme de 1948, à l’article 8 de la Convention européenne des droits de l’homme, et à l’article 17 du Pacte international relatif aux droits civils et politiques.

³⁸⁹ Le sigle RGPD signifie « Règlement général sur la protection des données » (en anglais : « General Data Protection Regulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l’Union européenne. Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel par les institutions, organes et organismes de l’Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE., en ligne : <<http://data.europa.eu/eli/reg/2018/1725/oj>>.

« découle du droit à la vie privée ou même du droit à la réputation³⁹⁰ ». Le droit au respect de la vie privée inclut le droit à l'intimité, le droit à l'anonymat, et le droit au secret et à la confidentialité³⁹¹. De cela découle le droit au contrôle des données personnelles³⁹².

Nous poursuivons le concept selon lequel la protection du nom d'une personne s'inscrit sous la notion du droit à l'anonymat, à l'égal de l'image et de la voix. Par conséquent, la protection du nom permet donc de s'approprier son identité et d'exercer un certain contrôle sur la diffusion non autorisée de son identité par son nom, dès que sa vie privée est menacée³⁹³. Dans le même sens, la reconnaissance du droit à la vie privée inclut impérativement le droit d'une personne de déterminer elle-même quand, comment et avec quelles précautions l'on diffusera ou non des renseignements personnels concernant cette personne³⁹⁴. Pour de multiples raisons, ce droit à l'autodétermination informationnelle peut s'apparenter à celui du droit à l'oubli étant donné que la personne reprend un certain contrôle sur l'information à son égard qu'elle choisit de rendre public ou de diffuser³⁹⁵. Or, les données à caractère personnel sont liées conceptuellement et juridiquement à la personne. La donnée n'est en effet rien de plus qu'une information corrélatrice à une personne physique identifiée ou qui peut être identifiée³⁹⁶ au sens de la notion du droit au respect de la vie privée. Le passage de l'identité des personnes à la donnée numérique à

³⁹⁰ Édith Deleury et Dominique Goubau, *Le droit des personnes physiques*, Cowansville, Yvon Blais, 2014, à la p 210

³⁹¹ *Ibid* à la p 213.

³⁹² *Ibid* aux pp 214-215.

³⁹³ *Ibid* à la p 213.

³⁹⁴ *Ibid* à la p 209.

³⁹⁵ Qu'est-ce que l'autodétermination informationnelle ? Pour la professeure de droit Astrid Epiney de l'Université de Fribourg, il s'agit de pouvoir de « déterminer qui utilise des informations nous concernant, qui les propage et à quelles fins ». Voir « L'autodétermination informationnelle : le nouveau défi des droits humains ? » (15 février 2017) en ligne : <<https://www.humanrights.ch/fr/pfi/droits-humains/sphere-privee/autodetermination-informationnelle>>.

³⁹⁶ L'article 2 (1) de la Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5 (Loi canadienne) définit la notion de données personnelles en ses termes : « tout renseignement concernant un individu identifiable ». En Europe, la Loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, JO, 16 novembre 2016, modifiée par ordonnance no 2018-1125 du 12 décembre 2018 stipule à son article 2 : « Constitue un fichier de données à caractère personnel tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

caractère personnel ne se produit que par l'intervention d'une manipulation technique³⁹⁷. Dans ce contexte, la donnée devient dorénavant un objet juridique spécifique intimement lié à la personne humaine, et non pas seulement une information virtuelle. Cependant, nonobstant les similitudes qui peuvent être établies, le droit à l'oubli numérique est un concept juridique qui se distingue de la notion du droit au respect de la vie privée, quoique cette dernière soit de portée générale et plus flexible. Selon Serge Gutwirth (professeur de droit de l'Université de Bruxelles), le droit à l'oubli numérique peut difficilement être élaboré à partir du droit à la vie privée étant donné que la majorité des informations que le droit à l'oubli s'efforce de protéger sont des informations déjà diffusées et publiques³⁹⁸.

Considérant la position de l'auteur Gutwirth, les informations en cause n'ont jamais fait partie du domaine privé de la personne, et c'est la raison pour laquelle le droit à l'oubli numérique devrait avoir comme assise le droit à l'identité de la personne. Dans ce contexte, le droit à l'oubli est un droit distinct : il voit à ce que chaque personne exerce un certain contrôle juridique sur son passé, et il comprend aussi les données à caractère personnel associées à la vie privée de la personne qui sont pourtant publiques et qui ont été publiées légalement ou non³⁹⁹.

2.3.6 Le droit à l'oubli numérique et la liberté d'expression

Subsidiairement, le droit à l'oubli numérique ne doit pas être confondu avec la liberté d'expression, alors que le droit à l'oubli porte sur des informations véridiques ou pas et légalement obtenues ou non, mais qui ne sont plus pertinentes ou d'actualité.

Pour sa part, le droit à la liberté d'expression est souvent invoqué pour faire obstacle au droit à l'oubli numérique, de crainte que ce dernier limite la liberté d'expression et l'intérêt journalistique pour l'information ainsi diffusée sur Internet ou sur d'autres médias. En effet, pour certains auteurs, le droit à l'oubli numérique a été associativement qualifié de

³⁹⁷ Loi 78-17 du 6 janvier 1978, JO, 16 novembre 2016, modifiée par ordonnance no 2018-1125 du 12 décembre 2018, art. 2.

³⁹⁸ Serge Gutwirth, « Beyond Identity ? », *IDIS-Identit in the Information Society* 2.2, (2009) 126.

³⁹⁹ Letteron, *supra* note 38 à la p 407.

« chose » et de « dangereux » par Sir Timothy John Berners-Lee (ingénieur britannique reconnu comme l'inventeur du World Wide Web : « www »), et récrié comme étant « profondément immoral » par Jimmy Wales (fondateur de Wikipédia). Selon le New York Times, la reconnaissance de ce droit par les tribunaux européens est une menace pour la liberté de presse et la liberté d'expression⁴⁰⁰.

Plus près de nous, dans une chronique publiée le 29 octobre 2019, Pierre Trudel (professeur de droit à l'Université de Montréal) exprime ses inquiétudes de la façon suivante :

La réglementation européenne est la plus avancée en matière de protection des données personnelles. Elle tend à s'imposer comme le standard mondial en la matière. Mais il est inquiétant que le droit de la protection des renseignements personnels européen soit si prompt à imposer la censure des informations publiques au lieu de renforcer les protections essentielles pour les informations relevant vraiment de l'intimité. Cela le rend non exportable dans les pays qui accordent de l'importance au droit du public à l'information⁴⁰¹.

Bien que le droit à l'oubli numérique soit déjà reconnu par plusieurs États, il entre en conflit direct, selon un certain courant de pensées juridiques, avec le droit à l'information du reste de la société, brimant de ce fait la liberté d'expression. Or, *a contrario*, selon certains auteurs, il est important de protéger les informations à caractère personnel contre la liberté d'expression, particulièrement sur Internet, car il ne faut pas que cette liberté rende les individus moins libres d'être eux-mêmes⁴⁰². Par conséquent, la personne ainsi visée par l'information demeure stigmatisée le reste de ses jours, et même sa descendance dans certains cas⁴⁰³. Mais plus encore, pour exister comme concept, le droit à l'oubli a obligatoirement fait l'objet de publication et de diffusion quelque part, journaux, revues,

⁴⁰⁰ Doug Beazley, « Le droit à l'oubli : Vie privée contre liberté d'expression », L'Association du Barreau canadien, (2018) à la p 1, (27 août 2018) en ligne : <<https://www.cba.org/Publications-Resources/CBA-Practice-Link/Business-and-Corporate/2018/Right-to-be-forgotten-sets-privacy-against-freedom?lang=fr-ca>> (Consulté le 16 août 2022).

⁴⁰¹ Pierre Trudel, « La censure en Europe », *Le Devoir*, 29 octobre 2019.

⁴⁰² Jeffrey A. Rosen, « Free Speech, Privacy, and the Web that Never Forgets », (2011) 9 *J Telecom & H Tech L*, 345.

⁴⁰³ Carter, *supra* note 19.

presse, plateformes numériques et réseaux sociaux, etc. C'est l'essence même de « l'oubli », tel que déjà vu au chapitre de sa définition.

Au vu de ce qui précède, nous considérons dès lors qu'il n'y a aucune violation de la liberté d'expression dans le fait de déréférencer des informations personnelles déjà publiées après un certain écoulement du temps. Selon nous, il s'agit ici d'un faux débat, basé sur une compréhension erronée de ce droit⁴⁰⁴.

⁴⁰⁴ C'est ce qui ressort de l'ensemble de notre étude sur la notion du droit à l'oubli numérique. La recherche d'un équilibre entre les différents droits fondamentaux, notamment, le droit à la protection de la vie privée, la liberté d'expression et le droit à l'information a fait l'objet d'une préoccupation intrinsèquement liée et incluse dans toutes les lois, règlements ou projets de Loi à l'oubli, droit à l'effacement ou sur le déréférencement des différents États susmentionnés.

CONCLUSION

Depuis les années 70, les technologies émergentes de l'information font leurs apparitions. Le concept de protection des données à caractère personnel se manifeste à ce moment-là, dans le sillon de celle de la vie privée, particulièrement en Europe. Dès 1978, la Loi française « informatique et libertés »⁴⁰⁵ est proclamée. Cette Loi donne une première protection juridique aux renseignements contenus dans les traitements automatisés de données personnelles. À compter des années 90, le développement des technologies numériques et particulièrement la place que prend l'Internet en matière de diffusion et captation de données entraînent une prise de conscience des enjeux juridiques liés à la protection de la vie privée dans le domaine numérique. Dans le même ordre d'idées, on observe un chevauchement dans le langage législatif, des deux notions de protection de la vie privée et de protection des données à caractère personnel. Dérivée sur le terrain de l'information numérique et des libertés fondamentales, la question de la protection juridique de la vie privée s'attribue de la revendication du droit à l'oubli qui, en apparence, se heurte légitimement à la liberté d'expression. Or, l'ensemble des lois ou projets de lois sur la protection des données ou renseignements personnels visité pendant cette étude est un reflet d'un subtil exercice d'équilibriste entre le droit à l'oubli et le droit à la liberté d'expression. La relation entre ces deux droits fondamentaux est complexe, mais dans le même temps ces deux droits peuvent être limités dans certaines circonstances prévues par la Loi et être nécessaires dans une société démocratique.

Cela signifie entre autres que les États démocratiques sont tenus de considérer d'adopter des mesures de protection du droit au respect de la vie privée en ligne, étant donné qu'il est essentiel pour que les personnes aient une confiance suffisante pour exercer librement leur droit à la liberté d'expression. En d'autres mots, la liberté d'expression et le droit au respect de la vie privée se renforcent mutuellement, mais entre parfois en opposition. Dans ce contexte, il est parfois plus compliqué de faire valoir un droit à l'oubli fondé sur le seul droit à la protection des données à caractère personnel, face à la liberté fondamentale qu'est la liberté d'expression dont relève le droit de la presse. En ce cas, le fait d'élever le droit à

⁴⁰⁵ Loi 78-17 janvier 1978, *supra* note 55.

l'oubli au niveau d'une manifestation intrinsèque de la protection de la vie privée, liberté fondamentale également garantie dans la plupart des traités internationaux⁴⁰⁶ des droits humains⁴⁰⁷, entraîne la recherche d'une nécessaire conciliation entre ces deux droits fondamentaux. Il ne faut pas perdre de vue que le droit à l'oubli est la sollicitation active d'une personne et porte sur des informations précises la concernant qui cherchent à faire oublier sur Internet par un déréférencement associé à son nom. Le nom de la personne est l'identité qui la définit et la représente au regard de la loi. D'ores et déjà, cette identité est devenue une donnée sur le Web représentant sa personnalité numérique. Alors que le traitement et le contrôle des données sont l'apanage des acteurs numériques privés.

Le droit à l'oubli est perçu comme l'alternative ultime de protection de la personne et de sa vie privée face à des pratiques numériques toujours plus invasives⁴⁰⁸, mais cet oubli volontaire, demandé par un individu, se heurte de front à l'appréciation des exploitants de moteur de recherche, plateformes numériques, etc., puisque c'est eux les acteurs privés qui décident au final. Ainsi, au-delà de la question du droit à l'oubli numérique, il n'appartient pas au GAFAM de réguler le traitement des données à caractère personnel qui nous appartiennent, mais au pouvoir étatique de faire prévaloir l'intérêt général par des mesures

⁴⁰⁶ Article 12 de la Déclaration universelle des droits de l'homme DUDH. Le 10 décembre 1948, les 58 États membres qui constituaient alors l'Assemblée générale ont adopté la Déclaration universelle des droits de l'homme à Paris au Palais de Chaillot (résolution 217 A (III)). Pour commémorer son adoption, la Journée des droits de l'homme est célébrée chaque année le 10 décembre. Article 17 du Pacte international relatif aux droits civils et politiques PIDCP. Article 8 de la Convention européenne, Articles 5, 9 et 10 de la Déclaration américaine des droits de l'homme, et Article 11 de la Charte africaine. Afrique - Charte africaine des droits de l'homme et des peuples du 17 juin 1981. Voir : *Déclaration universelle des droits de l'homme*, Rés AG 217A (III), Doc Off AG NU, 3è sess, supp n° 13, Doc NU A/810 (1948) 71 et *Pacte international relatif aux droits civils et politiques*, Rés AG 2200 (XXI), Doc off AG NU, 1496ième séance plénière, Doc NU A/RES/2200 (XXI) (1966).

⁴⁰⁷ Voir par ex. US Department of State, 2022 Country Reports on Human Rights Practices, April 2022.

Les rapports annuels des pays sur les pratiques en matière de droits de l'homme - les rapports sur les droits de l'homme - couvrent les droits individuels, civils, politiques et des travailleurs internationalement reconnus, tels qu'énoncés dans la Déclaration universelle des droits de l'homme et d'autres accords internationaux. Le Département d'État américain soumet au Congrès américain des rapports sur tous les pays bénéficiaires d'une assistance et de tous les États membres des Nations-Unies, conformément à la Loi sur l'assistance étrangère de 1961 et la Loi sur le commerce de 1974, en ligne : <<https://www.state.gov/reports-bureau-of-democracy-human-rights-and-labor/country-reports-on-human-rights-practices/>> (consulté le 16 août 2022).

⁴⁰⁸ Voir, par exemple, l'illustration qu'en donne François Pellegrini et André Vitalis dans leur article « L'ère du fichage généralisé ». François Pellegrini et André Vitalis, « L'ère du fichage généralisé », *Le Monde diplomatique*, (avril 2018) à la p 3, en ligne : <<https://www.monde-diplomatique.fr/2018/04/PELLEGRINI/58551>> (consulté le 16 août).

juridiques équitables sur le contrôle et le traitement desdites données. Avantagement, l'Union européenne a tracé le sentier, le Canada et le Québec ont suivi, sur le plan juridique pour offrir à leurs citoyennes et citoyens un certain contrôle sur leurs données personnelles. L'étude du droit américain, quant à lui, démontre que les perspectives d'évolution du droit à l'oubli restent très limitées, nonobstant le Projet de Loi Data Care Act⁴⁰⁹ initié par le sénateur Brian Schatz. Considérant, le premier amendement de la Constitution américaine de 1791, qui interdit explicitement au Congrès des États-Unis d'adopter des lois limitant la liberté d'expression et la liberté de presse. Mais qui est « journaliste » ou membre de la presse ? C'est une question à laquelle la Cour suprême des États-Unis résiste à répondre.

Bien que les tribunaux américains daignent de répondre à cette question, au Canada, la Cour fédérale, dans le renvoi du 8 juillet 2021⁴¹⁰, sous la plume de Mme la juge en Chef adjointe Gagné, exprime l'opinion sur la question « journaliste » invoquée par l'exploitant de moteur de recherche de la façon suivante : Même si certains contenus journalistiques s'affichent dans les résultats de recherche de Google, l'action de présenter ces résultats ne fait pas partie de la définition du journalisme a tranché la juge⁴¹¹.

Ainsi, nous soulignons en terminant, le droit à l'oubli doit être envisagé comme une notion juridique couvrant différents dispositifs de mise en œuvre concourant à la protection de la vie privée de la personne à travers ses données, favorisant la sécurité numérique de la personne et limite les intrusions informationnelles pernicieuses dans sa vie. Dans cette perspective tous azimuts des données numériques, le droit à l'oubli illustre les nouveaux enjeux juridiques et l'altération des droits fondamentaux auxquels sont confrontés les États et c'est ainsi que plusieurs de ceux-ci ont compris que ce vide juridique ne peut continuer.

⁴⁰⁹ Personal Data Online, *supra* note 311; Data Care Act of 2021, *supra* note 312.

⁴¹⁰ Renvoi relatif au titre du paragraphe 18.3 (1) de la Loi sur les Cours fédérales, *supra* note 347.

⁴¹¹ *Ibid* au paragraphe 89. Voir aussi la décision : A.T. c. Globe 24h. com, 2017 CF114.

BIBLIOGRAPHIE

Sources primaires

Législations internationales et nationales

CE, Décision-cadre 2008/977/JI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, (2008), JO, L 350.

CE, Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, (1995), JO, L 281.

CE, Résolution (CE) (73) 22 du Conseil de L'Europe comité des ministres du 26 septembre 1973 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé. (1973).

Charte canadienne des droits et libertés, partie 1, de la Loi constitutionnelle de 1983, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c11.

Charte du droit à l'oubli, 13 octobre 2013, Mieux protéger les données personnelles des internautes, (2013) Paris, Fr, 13 octobre 2013.

Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505

Déclaration universelle des droits de l'homme, Res AG 217A III, Doc off AG NU. 3^e sess., supp no. 13, Doc NU a/810 (1948) 71.

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. 2510-2523.

Gramm Leach Bliley Act., Nov. 12, 1999, Public Law 106-102.

Health Insurance Portability and Accountability Act of 1996 (HIPAA). Public Law 104-191.

Loi no. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF, 6 août 2004.

Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000-C-5.

Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000-C-5, Loi mise à jour le 4 avril 2022.

Pacte international relatif aux droits civils et politiques, 16 décembre 1966, 999 RTNU 1057 (entrée en vigueur : 23 mars 1976).

Privacy Act of 1974 as amended, 5 U.S.C 552 A.

Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données et abrogeant le règlement (CE) no. 45/2001 et la décision no. 1247/2002/CE, en ligne : <http://data.europa.eu/eli/reg/2018/1725/oj>.

S. 919, Data Care Act of 2021, 1^{ère} sess., To establish duties for online service providers with respect to end user data that such providers collect and use, 117th Congress, March 23, 2021, en ligne: [congress.gov/bill/117th-congress/senate-bill/919/test](https://www.congress.gov/bills/117/congress/senate-bill/919/test).

UE. Charte 2007/C 303/01, Conseil de l'Union européenne, Charte des droits fondamentaux de l'Union européenne, (2007) JO. L c. 303/1.

UE. Charte 2012/C 326/02, du Parlement européen et du Conseil du 26 octobre 2012, Charte des droits fondamentaux de l'Union européenne, (2012) JO, L c. 2012.

UE. Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE, (2016) JO. L 2016/679.

UE. Règlement 2018/302 du Parlement européen et du Conseil, du 28 février 2018. Visant à contrer le blocage géographique injustifié et d'autre forme de discrimination fondée sur la nationalité, le lieu ou résidence ou le lieu d'établissement des clients dans le marché intérieur. (2018) JO. L, 601.

US. Bill of Right (1789), Joint Resolution of Congress du 25 September 1789, proposing 12 Amendment of the U.S. Constitution, (1789) amendments ratified December, 151791, en ligne: [archives.gov/founding-docs/bill-of-rights-transcript](https://www.archives.gov/founding-docs/bill-of-rights-transcript).

US. Electronic Communications Privacy Act (ECPA) de 1986.

US. Privacy Act (ECPA) de 1986.

Déclaration américaine des droits de l'homme 2 mai 1948, 999 RTNU 171. (entrée en vigueur : le 19 juillet 1978).

Charte africaine des droits de l'homme et des peuples du 27 juin 1981, 1520 RTNU 217 (entrée en vigueur : 21 octobre 1986).

Charte des droits et libertés de la personne 1977 C-12 des lois refondues du Québec.

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ, c.p.39.1.

Loi sur le système correctionnel et la mise en liberté sous condition, L.C. 1992, ch. 20.

Projets de loi

PLC-11, Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le tribunal de protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois, 2^e session 43^e parl., 2020. Projet de Loi C-11 (première lecture).

No. 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, 2^e sess., 42^e Légis. 2021, adoptée par l'Assemblée nationale du Québec le 22 septembre 2021.

Jurisprudences

Goyette c. Rodier (1889) 20 R.L. 108, 110 (C. Rev).

R c Dymont (1988) 2RCS 417.

TGI Paris, 20 avril 1983, *M.c. Fillipacchi et Cogedipresse*, JCP 1983kk, II, 20434.

CJUE, Grande Chambre, 13 mai 2014, *Google Spain SL et Google Inc. C. Agencia Espanola de Proteccion de Datos et Mario Costeja Gonzalez*, C-131/12.

Tribunal de district d'Amsterdam, C/13/636885/HA_KK_17-30/, jugement du 19 juillet 2018, publication 18 décembre 2018.

Cour d'Appel d'Amsterdam, 200.248.187/01, jugement du 7 avril 2020, publication 6 juillet 2020, en ligne : <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHAMS:2020:1270>

CJUE, 24 septembre 2019 aff.C_136/17.

CJUE 24 septembre 2019, aff.C-507/17.

Délibération SAN-2019-001 du 21 janvier 2019.

Chambre contentieuse, Décision quant au fond 37/2020 du 14 juillet 2020, France.

No. De dossier : Dos-2019-03780, Autorité de protection des données. X C. Google.

Cox Broadcasting Corp. c. Cohn (1975) 42 US. 469.

Oklahoma Publishing Co. c. District Court for Oklahoma County, (1977), 430 US 308.

Smith c. Daily Mail Publishing Co., (1979) 443 U.S. 97.

Florida Star c. B.J.F. (1989) 419 U.S. 524.

Irwin Toy Ltd c. Québec (Procureur général), 1989 1 RCS 927.

Ford c. Québec (Procureur général) 1988 2 RCS 712, paragraphe 59.

Société Radio-Canada c. Canada (Procureur général) 2011 1 RCS 19.

Montréal (Ville) c. 2952-1366 Québec Inc. 2005 3 RCS 141.

Dagenais c. Société Radio-Canada, 1994 3 RCS 835.

Rocket c. Collège Royal des chirurgiens-dentistes de l'Ontario, 1990 2 RCS 232.

R. c. Vidéofliqué, 1984, 14 D.L.R. (4th) 10.

Aubry c. Édition Vice-Versa Inc., 1998 1 RCS 591.

Hill c. Église de scientologie de Toronto, 1995 2 RC 1130.

Grant c. Toronto Corp, 2009 3 RCS 640, paragraphe 51.

Google inc. c. Equustek Solutions Inc. 2017 1 RCS 824.

Google inc. v Equustek Solutions Inc., Case no 5.17-CV-04207-EJD.

Equustek Solutions Inc. c Jack 2018 BCSC 610 (CanLII) para 19.

Douez c. Facebook Inc. 2017 1 RCS 751.

C.L. c. BCF Avocats d'affaires, 2016 QCCA 114.

A.T. c. Globe 24h. com, 2017 CF114.

Sources secondaires

Doctrine, ouvrages généraux et articles

- Ausloos, Jeff. « the « Right to be Forgotten » Wort remembering? » For Forth coming computer Law & Security Review 2012, no4, 1156-11170.
- Ayed, Camille. « L'arrêt Google Spain c. AEPD : Analyse comparative du droit à l'oubli numérique en Europe et aux États-Unis », 2017, MBDE.
- Beazley, Doug. « Le droit à l'oubli : Vie privée contre liberté d'expression », L'Association du Barreau canadien, 2018, p. 1. En ligne : www.cba.org/Publications-Ressources/CBA-Pratice-Link/Business-and-Corporate/2018/Right-to-be-forgotten-sets-privacy-against-freedom?lan.
- Benabou, V.L. et J. Rochfeld. Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique? Dallos, no. 25, 10 juillet 2014, pp. 1476-1481.

- Benyechlef, Karim et Pierre-Luc Déziel. *Le droit à la vie privée en droit québécois et canadien*, Montréal, Éditions Yvon Blais, 2018.
- Blanchette Françoise et Deborah Johnson. *Data Retention and the Panoptic Society: The social Benefits of Forgetfulness*, manuscript, available online <http://www.rpi.edu/~blanc>(last visit April 20, 2007).
- Boffey, Daniel. « Dutch Surgeon Wins Landmark Right to be Forgotten Case », *The Guardian*, 21 janvier 2019, en ligne : www.worldcat.org/issn/0261-3077&lang=fr; www.theguardian.com/technology/2019/jan/21/dutch-surgeon-wins-landmark-right-to-be-forgotten-case-google.
- Boizard, Maryline. *Le Temps, le droit à l'oubli et le droit à l'effacement*, Les Cahiers de justice, vol. 4, no. 4, 2016 p. 620.
- Castells, Manuel. *The Internet Galaxy*, Oxford, Oxford University Press, 2001.
- Carter, Edward L. "Argentina's Right to be Forgotten", (2013) 27 *Emory Int'l L. Rev.* 23, à la p 30 en ligne: <<https://scholarlycommons.law.emory.edu/eilr/vol27/iss1/3>>
- Charrière-Bournarzel, Christian. *Propos autour d'Internet : l'histoire de l'oubli*, Gazette du palais, 21 avril 2011 no. 111, Paris, à la p.6.
- Checola, Laurent. *Droit à l'oubli sur Internet : une charte signée sans Google ni Facebook*, Le monde.fr.13 octobre 2010.
- Claeyssen, Yan. *Oublions le « droit à l'oubli » numérique !* La tribune (France) no. 4465 p. 16, 6 mai 2010.
- Cofone Ignacio et Pierre-Luc Déziel. *The Right to Be Forgotten, A Canadian and Comparative Perspective*, Montréal, Ignacio N. Cofone, 2020.
- Cornu, Gérard. *Dir., Vocabulaire juridique*, 8^e éd., Paris, Presse universitaire de France, 2018.
- De Hert Paul et Serge Gutwirt. *Data protection in the case Law of Strasbourg and Luxemburg: Constitutionality in action*, 2009 pp. 3-44.
- De Terwangne, Cécile. « Internet Privacy and the Right to Be Forgotten/Right to Oblivion » (2012) VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet" [monograph online]. *IDP. Revista de Internet, Derecho y Política*. No. 13, pp. 109-121. UOC.
- Dechenaud, David. *Le droit à l'oubli numérique. Données nominatives approche comparée*, Bruxelles, Larcier, 2015.
- Deleury Édith et Dominique Goubau. *Le droit des personnes physiques*, Cowansville, Yvon Blais, 2014.

- D'Elia, Helena et Nathalie Dollez. Exil et violence politique, les paradoxes de l'oubli, Toulouse, Éres, 2019.
- Delwaide Karl et Antoine Guilmain. « Le Droit à l'oubli se fait tailler un nouveau costume trois pièces au Canada ? Du Québec à la Colombie-Britannique », 2017 En ligne : <unik.caij.qu.ca>.
- Dreyfus, Stéphane. « La présidente de la Commission nationale de l'informatique et des libertés (CNIL) se réjouit de la décision européenne imposant un droit à l'oubli numérique, nouvelle arme à disposition des citoyens », *La Croix*, no. 39983, p11, 12 septembre 2014.
- Duton, Jean Christophe et Virginie Becht. « Le droit à l'oubli numérique : Un vide juridique? » 2012 Journal du Net. En ligne : [http : www.journaldunet.com/ebusiness/45246/le-droit-a-l-oubli-num.rique-un-vide-juridique.shtml](http://www.journaldunet.com/ebusiness/45246/le-droit-a-l-oubli-num.rique-un-vide-juridique.shtml).
- Enis Van, Q., « Droit des médias, liberté d'expression et nouvelles technologiques », RDTI, 2015, no 59-60.
- Epiney, Astrid. L'autodétermination informationnelle : le nouveau défi des droits humains? Suisse 2017. En ligne : [https ://www.humanrights.ch/fr/pfi/droits-humains/spere-privee/autodetermination](https://www.humanrights.ch/fr/pfi/droits-humains/spere-privee/autodetermination).
- Ferron D et C. Cassagnabèr. « Nouveaux développements dans l'affaire Google Inc. C. Equustek Solutions Inc. », 23 janvier 2018. En ligne : <Langlois.ca/nouveaux-developpements-dans-laffaire-google-inc-c-equustek-solutions-inc/>.
- Gardner, John. *Law as a Leap of Faith: Essays on Law in General*, Oxford, 2012.
- Gomes De Andrade, Norberto Nuno. « Oblivion: The Right to be Different...from Oneself Reproposing the Right to be Forgotten », (2012) *I.D.P.* 13.
- Gratton, Louis-Philippe. *The latest consolidated version of the Regulation with corrections by Corrigendum, OJ L 127, 23.5.2018*.
- Gutwirth, Serge. « Beyond Identity? », *IDIS-Identity in the Information Society 2.2*, 2009, p. 126.
- Hass, Gérard. Guide juridique du RGPD, Édition ENI, avril 2018.
- Jongen J. et A. Strowel. « Section 2. Droit à l'oubli et à l'anonymat », dans *Droit des médias et de la communication*, Bruxelles : Éditions Larcier, 2017.
- Koops, Bert-Japp. Forgetting Footprints, Shunning Shadows. A Critical Analysis of the « Right to be Forgotten » in big data practice, (2011) 8 (3) *Issue 229, 240*.
- Lagane, Christophe. Google et Facebook oublient la charte du droit à l'oubli numérique, silicon.fr.14octobre 2010.
- Laurent, Alexandre. Publicité en ligne : une charte pour le « droit à l'oubli » Clubic, 1^{er} juin 2018.

- Letteron, Roseline. *Le droit à l'oubli (1996)*, 385, *Revue de droit public*, 391.
- McNealy, Jasmine E. The Emerging Conflict between Newsworthiness and the Right to be Forgotten, (2012) 39(2) N.K.L.R. 119.
- Negroponte, Nicolas. *Being Digital*, New York, Vintage Books, 1996.
- Nerbonne, Sophie. « Le Groupe de l'article 29 ». *LEGICOM* 1, 2009, pp.37-46.
- Nguyen, Benjamin. Professeur à l'INRIA informaticien. Sans difficulté sur la faisabilité technique du droit à l'oubli et au référencement, 19 janvier 2015.
- Nietzsche, Friedrich. *Considérations inactuelles, II*, « De l'inconvénient et de l'utilité pour la vie de l'histoire », 1874, tr. Fr. Pierre Rusch, Folio essais, 1992.
- Prasser, William Lloyd. Privacy, vol. 48, *California Law Review* 1960, p.383.
- Perotti, E. «The European Ruling on the Right to be Forgotten and its Extra-EU Implementation», December 2015. En ligne : <https://papers.ssrn.com/so13/DisplayAbstractSearch.cfm>.
- Pellegrini François et André Vitales. L'ère du fichage généralisé, *Le monde diplomatique* avril 2018, p.3, <https://www.monde-diplomatique.fr/2018/04PELLEGRINI/58551>).
- Rosen, Jeffrey A. "Free Speech, Privacy, and the Web that Never Forgets" 9 *Journal on télécommunication & High Law*, 345.
- Rees, Marc. « Droit au déréférencement : les critères de la CNIL pour se faire oublier sur Google » (<http://www.nextinpact.com/news/91147-droit-au-dereferencement-criteres-cnil-pour-se-faire-oublier-sur-google.htm>), CNIL, 2014.
- Roques-Bonnet, Marie-Charlotte. *Le droit peut-il ignorer la révolution numérique?* Paris : Michalon, 2010.
- Trudel, Pierre. « La censure en Europe », 2019, *Le devoir*, 29 octobre 2019.
- . L'oubli en tant que droit et obligation dans les systèmes juridiques civilistes, 2016, notes : <https://pierretrudel.openum.ca/files/sites/6/2016/08NotesoubliREV-1.pdf>.
- Viktor Mayer-Schoenberger, et Mayer-Schoenberger. Viktor, utile : l'art d'oublier à l'ère de l'informatique omniprésente (avril 2007). Document de travail du KSG no RWP07-022, disponible sur SSRN : <https://ssrn.com/abstract=976541>.
- Wagner Mike et Yun Li-Reilly. «The Right to Be Forgotten» (2014), *The Advocate*, 76(6), 823-829.
- Walker, Robert Kirk. the right to be Forgotten, 2012, 64 (101) H.L.j 214.
- Warren, Samuel. Louis Brandeis, the right to privacy, *Harvard Law*, Vol. 4, 1890, pp. 193-220.

Zick, Timothy. *Clouds, caméras et ordinateurs : le premier amendement et lieux publics d'un réseau*, 59 FL, L. Recueil, 1 (2007) p 263-267.

Lexique juridique

Cornu, Gérard. dir., *Vocabulaire juridique*, 8^e éd., Paris, Presse universitaire de France, 2018.

Dictionnaire Orthodidacte, 2022, en ligne :
<<https://dictionnaire.orthodidacte.com/article/definition-gafam>>.

Documentation Internationale et nationale

Commission nationale de l'informatique et des libertés de France (CNIL), *Rapport d'activité 2013*, 34^e Rapport annuel 2013, Paris, CNIL, 2013.

Commission européenne, Bruxelles, *Réforme globale de la directive 1995*, Com (2012) 11 final. 2012/0011/cod. Bruxelles, Parlement Européen et du Conseil, 2012

Commissariat à la protection de la vie privée du Canada, selon le commissaire à la protection de la vie privée, des améliorations s'imposent pour protéger la réputation en ligne, 26 janvier 2018, en ligne : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2018/nr-_180126/.

Commissariat à la protection de la vie privée du Canada, *Projet position du Commissariat sur la réputation en ligne*, 26 janvier 2018, en ligne : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-la-reputation-en-ligne/pos_or_201801/.

Commissariat à la protection de la vie privée du Canada, *Communiqué du 26 janvier 2018*, selon le commissaire à la protection de la vie privée, des améliorations s'imposent pour protéger la réputation en ligne : https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2018/nr-c_180126/

Commissariat à la protection de la vie privée du Canada, *Rapport de conclusions en vertu de la LPRPDE no. 2019-002*, 25 avril 2019 (Facebook Inc.).

Le commissaire à la protection de la vie privée du Canada a soumis un renvoi en vertu du paragraphe 18.3 (1) de la Loi sur la Cour fédérale, LRC 1985, CF-7, qui permet aux offices fédéraux de renvoyer à la Cour, à n'importe quelle étape de ses procédures, toute question de droit, de compétence ou de pratique et procédure.

Commission d'accès à l'information du Québec- Espace évolutif – *Projet de loi 64* <https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/#:~:text=Sanctionn%C3%A9e%20le%2022%20septembre%202021,technologique%20d'aujourd'hui>.

Consumer Watch dog sur leur site, en date du 7 juillet sur le sujet : « *Google's Failure To Offer 'Right to Be Forgotten' In United States is Unfair And Deceptive, Consumer Watchdog Tells Federal Trade Commission in Complaint* » (*L'échec de Google d'offrir un « droit à l'oubli » aux États-Unis est déloyal et trompeur, dit le Consumer Watchdog à la Federal Trade Commission dans sa plainte*): www.consumerwatchdog.org/newsrelease/google%E2%80%99s-failure-offer-%E2%80%98right-be-forgotten%E2%80%99-united-states-unfair-and-deceptive-consumer

Portail du Gouvernement, « Charte du droit à l'oubli numérique : mieux protéger les données personnelles des internautes », le monde. Fr. 13 octobre 2010.